IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

CARLTON TECHNOLOGIES, INC.,	)	
	)	
Plaintiff,	)	Case No. 07 C 06757
	)	Judge Coar
v.	)	Magistrate Judge Mason
	)	
JEFFREY GRAFSTEIN	)	
and BIZ 120, INC.,	)	Trial by Jury Demanded
	)	
Defendants.	)	

INDEX OF EXHIBITS IN SUPPORT OF
PLAINTIFF'S MOTION FOR A PRELIMINARY INJUNCTION

Exhibit	Description
Exhibit A	Declaration of Ryan Bracken
Exhibit B	Jeffrey Grafstein Employment Agreement
Exhibit C	Complaint for Injunction and Other Relief
Exhibit D	Unpublished Decisions

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

CARLTON TECHNOLOGIES, INC.,	)	
	)	
Plaintiff,	)	Case No. 07 C 06757
	)	Judge Coar
v.	)	Magistrate Judge Mason
	)	
JEFFREY GRAFSTEIN and BIZ 120, INC.,	)	Trial by Jury Demanded
	)	
Defendants.	)	

DECLARATION OF RYAN BRACKEN

I, Ryan Bracken, declare as follows:

1. I am the founder, owner, and President of Plaintiff Carlton Technologies, Inc. ("Carlton").

2. Founded in 1998, Carlton is a leader in providing and servicing refurbished wireless data collection devices, bar code scanners, and related hardware for commercial clients throughout the United States, Canada, and Europe.

3. Carlton has three sales professionals who are devoted full-time to developing new business opportunities and servicing existing customers. Carlton has spent approximately eight (8) years and thousands of dollars developing a confidential customer list.

4. At a cost in excess of $500,000 and over the course of several years, Carlton has compiled a database containing critical confidential information about its customers and prospective customers. Information within this database includes key contacts and decision makers; historical purchase information for each customer; a communication log identifying each communication with the customer reflecting their past, present, and future purchasing, selling, and maintenance needs; pricing strategies; profitability; gross and net profit margins;

specific customer installation platforms detailing all equipment and accessories they used in the past and present; and each customer's plans for future purchases and maintenance. This information is accessible on Carlton's secured computer network.

5. The information within this database is not available publicly and cannot be duplicated without a substantial amount of time and effort.

6. Carlton has also expended a great deal of time and money developing confidential pricing strategies and business plans. Pricing strategies are created and based upon each opportunity as it has been presented throughout the eight year period Carlton has been in the industry. The pricing strategies are customized for each account and customer. They are crucial in keeping Carlton competitive. The pricing strategies allow Carlton a competitive advantage, which is required to grow the business by winning new accounts and maintaining existing customers. The strategies have been developed throughout the years using the information entered into and contained within the database. All business plans are developed by a team of individuals, including but not limited to myself, acting as the President and Chief Executive Officer, the Chief Financial Officer, and various marketing teams. Developing these confidential business plans keeps Carlton competitive in the industry.

7. In its computer systems, Carlton also maintains numerous files titled "electronic price ordering guides" or "epog's." Epog files contain a variety of information about specific products, including part numbers, part descriptions, list prices, and distribution prices. Carlton has compiled the epog files over the course of several years. This information is not available to the public now and has not been for many years.

8. Carlton has implemented several strict security measures to ensure that its confidential information and trade secrets are not used or disclosed outside of Carlton or outside of the key employees with whom such information is shared.

9. All Carlton computer systems are password protected with access limited on a need-to-know basis. The cabinets, desk drawers, and offices where confidential documents are retained are not open to persons who are not employed by Carlton. Access to the system is further limited based on each individual's job duties and responsibilities.

10. All employees of Carlton are required to sign a confidentiality agreement in which they acknowledge the confidential nature of Carlton's information, agree not to disclose such information to the detriment of Carlton, and agree to return such information to Carlton upon termination of employment.

11. Carlton's Employee Policy Handbook states that "[a]ny computer hardware, software, e-mail, voice mail … or other electronic equipment … is expected to be used solely for the conduct of company business during work hours. Any use of such equipment for personal purposes of any kind must be approved in advance by your supervisor." A true a correct copy of portions of the Employee Policy Handbook is attached hereto as Exhibit 1.

12. Carlton employees do not have an expectation of privacy in their email or other electronic media. The Employee Policy Handbook states "[y]ou should understand that management may intercept, monitor, copy, review, or download any communications or files that are sent, received, or stored on our systems."

13. I hired Defendant Jeffrey Grafstein ("Grafstein") in February 2002 as a Senior Account Executive and Director of Wireless Data Collection Devices.

14. In connection with his hiring, Grafstein signed an Employment Agreement, including a confidentiality provision and a return of property upon termination provision. A true and correct copy of the Agreement is attached hereto as Exhibit 2. The Agreement also states that "all books, records, files, forms, reports, accounts, papers and documents relating in any manner to the Employer's business ... whether prepared by Employee or anyone else, are the exclusive property of the Employer."

15. In connection with his position, Grafstein had access to Carlton's most confidential information and trade secrets. He had access to this information on his company issued laptop as well as remotely from his personal computer.

16. I discovered from the Illinois Secretary of State's website that in December 2006, Grafstein incorporated Biz 120, Inc. ("Biz 120") in the State of Illinois to directly compete with Carlton.

17. Biz 120 has promoted itself as providing the same services as Carlton, including actively buying, selling, and repairing a broad range of technology. This technology includes hand held scanners, imagers, and wireless data collection terminals. Biz 120 also repairs scanners and other wireless devices. Information from Biz 120's website is attached hereto as Exhibit 3.

18. In late 2007, Carlton conducted an investigation into Grafstein's use and misappropriation of certain documents belonging to Carlton. The investigation was conducted over the course of a few months beginning in September 2007. I issued a directive to various Carlton employees and independent contractors to begin an investigation into Grafstein's activities.

19. The investigation consisted of, among other things, reviewing Grafstein's company issued laptop, computer hard-drive, Carlton's network server, and Carlton's internet based systems and applications.

20. The investigation revealed that on a single day in October 2006, while still employed by Carlton, Grafstein accessed hundreds of files in Carlton's computer systems containing Carlton's confidential information.

21. We discovered that these files included Carlton's business plan outline and information about numerous Carlton accounts and Carlton customers, including order history as well as preferred procedures for orders. Grafstein also accessed Carlton's confidential gross profit margin information by product and confidential information regarding customer purchases, including the legal requirements for certain contracts, pricing, and quantity information.

22. Grafstein had no legitimate business justification for accessing all of these files on one particular day.

23. During the investigation, we also discovered that, prior to his resignation, Grafstein also improperly attached a portable media device to Carlton's company issued laptop and downloaded confidential Carlton documents to this external media storage device.

24. The documents Grafstein downloaded included a "Price Guide." This document, labeled confidential, contains confidential product and pricing information, including list price, distributor price, and Carlton's sales price.

25. Grafstein also accessed Carlton's confidential database with his personal computer after hours. On multiple dates, Grafstein logged off of his company issued laptop and logged back on to the confidential database via his personal laptop or home computer just minutes later.

26. Grafstein had no legitimate business justification for logging into Carlton's confidential database with his personal computer or attaching his portable media device and downloading Carlton confidential information.

27. Grafstein resigned from Carlton in February 2007.

28. Carlton did not learn of Grafstein's activities and theft of this information until late 2007.

29. Carlton spent in excess of $5,000 investigating Grafstein's improper use of Carlton's computer systems.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on January 25, 2008.

Ryan Bracken

EXHIBIT 1

CARLTON
technologies, inc.

ELECTRONIC COMMUNICATIONS

Responsible Use of Equipment, e-mail, and Internet
Any computer hardware, software, e-mail, voice mail, Internet, or other electronic equipment or service made available to employees is expected to be used solely for the conduct of company business during work hours. Any use of such equipment for personal purposes of any kind must be approved in advance by your supervisor, done on your own time, and conducted in a responsible manner. It must not result in any additional expense to the company, any possible embarrassment or harm to the company, or any loss in productivity with regard to your work.

Specifically, if the Company subscribes to any electronic services on an unlimited usage basis, we do not object if you use these services for personal business before or after work hours or during your lunch break so long as you have the approval of your supervisor and do so in a responsible manner. However, if the Company is charged in any way for time used, you may not use these services for anything other than company business. Under no circumstances should you use these facilities for any personal purpose during the hours you are expected to be working. You may not use the company e-mail or Internet address for personal messages which might mistakenly be interpreted as statements from the company.

Prohibited Content
Use of all electronic systems will be held to the same standard as other business communications, including compliance with our antidiscrimination and antiharassment policies. Remember that what one person finds humorous might be offensive to others. Also, do not send any materials of a sensitive or confidential nature, which might be intercepted by third parties. Do not put anything in an electronic message that you would not want published or made part of a permanent record. You should notify management of any inappropriate materials that you receive or observe.

Copyrighted Materials
We specifically prohibit the illegal use of any type of copyrighted material -- i.e., without purchasing it or securing written permission from the copyright owner. Examples are music, videos, software, or any type of printed, audio, or visual materials that you do not have the legal right to use. Such illegal use or even possession can create serious liability for both you and the company.

No Expectation of Privacy
You should understand that management may intercept, monitor, copy, review, or download any communications or files that are sent, received, or stored on our systems. Compliance with these policies is a condition of your employment. Failure

EXHIBIT 2

EMPLOYMENT AGREEMENT

This Employment Agreement ("Agreement") is entered into as of February 21st, 2002 by and between Carlton Technologies, Inc. ("the Employer"), 2000 W. Fulton Street, Chicago, Illinois 60612, and Jeff Grafstein ("the Employee").

A. Employer is engaged in the business of purchasing, reconditioning and selling product scanners, cash registers and similar devices used at the point of sale in the retail industry and performing services such as refurbishing equipment for others; and

B. Employer has invested a substantial amount of time and resources in developing its business and marketing techniques and in obtaining and maintaining its client and referral base and Employer desires to protect its confidential information and confidential programs and its client base; and

C. Employer desires to retain the services of the Employee and for Employee to assist Employer in developing and maintaining its client base and its business; and

D. Employee is willing to be employed by Employer.

Therefore, the parties agree as follows:

1. **Employment.** Employer shall employ Employee as a Sr. Account Executive and Director of Wireless Data Collection and Scanning Devices. Employee's duties are set forth on Exhibit "A". Employee accepts and agrees to such employment, subject to the general supervision, advice and direction of Employer and the Employer's supervisory personnel. Employee shall also perform such other duties Employer requests Employee to perform. Employee shall also follow all rules of Employer.

2. **At Will Employment.** Your employment with Employer is entered into voluntarily, and you are free to terminate your employment at any time, with or without a reason. Similarly, the Employer has the right to terminate your employment at any time, with or without a reason. Although the Employer may choose to terminate your employment for cause, cause is not required. This is called "at-will" employment. While it is expected that our working relationship will be mutually satisfactory, neither you, nor the Employer, have entered into any express or implied contract of employment for any specified period of time. No one other than the President of the Company that employs you can enter into an agreement for employment for a specified period of time, or make any agreement or representation contrary to the at-will employment policy. The Employer's policy of at-will employment can be changed only in a writing signed by the President of the Company that employs you.

3. **Best Efforts of Employee.** Employee agrees to perform faithfully, industriously, and to the best of Employee's ability, experience, and talents, all of the duties that may be required by the express and implicit terms of this Agreement, to the reasonable satisfaction of Employer. Such duties shall be provided at such place(s) as the needs, business, or opportunities of the Employer may require from time to time.

4. **Compensation of Employee.** As compensation for the services provided by Employee under this Agreement, Employer will pay Employee such compensation as reflected on Exhibit "A". Payments will be made at such payment cycles as the Employer shall determine. Upon termination of this Agreement, payments under this paragraph shall cease, provided, however, that the Employee shall be entitled to payments for periods or partial periods of work that occurred prior to the date of termination and for which the Employee has not yet been paid. Accrued vacation time will be paid in accordance with state law and the Employer's customary procedures.

5. **Absence from Work and Tardiness.** Employer understands that family emergencies and sickness occur which may occasionally require that Employee miss work. In such an event, it is expected that

Employee provide Employer with as much notice as possible of an absence due to an emergency or sickness. Employer may require, in Employer's sole discretion, a note from a physician to verify an illness. Regular full-time employees are entitled to five (5) sick days with pay per year. Sick days are not vacation days and are only to be utilized in the event of a family emergency or an illness which renders Employee incapable of attending work. Sick days may not be carried over from one year to another and Employee is not entitled to receive any pay for unused sick days. Unexcused or excessive absences are grounds for immediate dismissal. Each Employee has a start time. Employee is expected to be at work and ready to begin working at his/her customary start time. Excessive tardiness is grounds for immediate dismissal.

6. **Reimbursement for Expenses in Accordance with Employer Policy.** The Employer will only reimburse Employee for approved out-of-pocket expenses in accordance with Employer policies in effect from time to time.

7. **Recommendations for Improving Operations.** Employee shall provide Employer with all information, suggestions, and recommendations regarding Employer's business, of which Employee has knowledge, that will be of benefit to Employer.

8. **Confidentiality.** Employee recognizes that Employer has and will have information regarding the following:

- products
- margins
- discounts
- business affairs
- marketing plans
- prices
- costs
- future plans
- costs
- customer lists

and other vital information (collectively "Confidential Information") which is valuable, special and unique assets of Employer. Employee agrees that the Employee will not at any time or in any manner, either directly or indirectly, divulge, disclose, or communicate in any manner any Confidential Information to any third party even if such Confidential Information was developed by the Employee during the term of employment of Employee or obtained during or after the term of employment of Employee, without the prior written consent of the Employer. Employee will protect the information and treat it as strictly confidential. A violation by Employee of this paragraph shall be a material violation of this Agreement and, in the event of a violation, Employer shall be entitled to both legal and equitable relief. Employee acknowledges and agrees that the sale or unauthorized use or disclosure by Employee of any Confidential Information of the Employer constitutes unfair competition, and during the term of his employment with the Employer and thereafter, Employee will not engage in any unfair competition with the Employer by directly or indirectly using the Confidential Information, nor will Employee directly or indirectly disclose, publish or make use of, nor authorize anyone else to use Confidential Information or any information or knowledge which in any way relates to the business, product or services of the Employer.

9. **Other Employees.** Employee agrees for a period of two (2) years after the end of his/her employment with the Employer that Employee will not solicit for Employee's benefit or for the benefit of another business or enterprise any person employed by the Employer within six (6) months of Employee's last date of employment.

10. **Non-Solicitation.** In order to protect Employer's longstanding business relationships, Employee agrees that he/she will not, for a period of one hundred and eighty days (180) after his/her employment with Employer ceases for any reason, solicit, directly or indirectly, whether for Employee or as an officer, director, employee, agent or independent contractor of another, for purposes of performing any services or furnishing any equipment of a type similar to that provided by Employer to any client of Employer for whom Employee had contact with during the term of Employee's employment or any person or entity that Employee learned about or obtained any information concerning said person or entity's need for equipment or services as a result of Employee's employment.

"Client," as used herein, shall mean any person or entity for whom Employer performed services or sold equipment within a twelve (12) month period prior to the termination of employee's employment.

11. Injunction. Employee agrees that should he/she breach any provision of this Agreement, Employer will suffer irreparable injury and will have no adequate remedy at law. In such an event, Employer shall be entitled to obtain temporary, preliminary and permanent injunctive relief, without bond in any proper court which shall include the Circuit Courts of Cook County, Illinois. In addition to the above, should Employee breach this Agreement, Employer's rights shall be cumulative and Employer may also seek recovery of money damages as well. Thus, all covenants of this Agreement shall survive the termination of Employee's employment.

12. Records Belong to Employer. All books, records, files, forms, reports, accounts, papers and documents relating in any manner to the Employer's business, vendors, suppliers, or customers, whether prepared by Employee or anyone else, are the exclusive property of the Employer and shall be returned immediately to the Employer upon termination of employment or upon the Employer's request at any time. This excludes items that belonged to the Employee prior to beginning his/her employment with Employer.

13. Employee's Inability to Contract for Employer. Employee shall not have the right to make any contracts or commitments for or on behalf of Employer without first obtaining the express written consent of Employer.

14. Vacation. The Employer provides vacation time for Regular Full-Time employees and expects employees to take time away from work to renew their energy and enjoy some leisure activities with family or friends. The amount of vacation time is reflected on Exhibit "A". You may not receive pay in lieu of vacation, except as required by law upon termination of your employment or as Employer shall agree. In order to insure that Employer is sufficiently staffed to continue orderly operations, vacation time must be pre-approved at least two weeks in advance. Employer may, in its sole discretion, not approve a request for vacation time due to scheduling problems or other business demands.

15. Holidays. Employee shall be entitled to the following holidays with pay during each calendar year:

- New Year's Day
- Independence Day
- Thanksgiving Day
- Memorial Day
- Labor Day
- Christmas Day

16. Compliance With Employer's Rules. Employee agrees to comply with all of the rules and regulations of Employer.

17. Return of Property. Upon termination of employment, the Employee shall deliver all property (including keys, records, notes, data, memoranda, models, and equipment) that is in the Employee's possession or under the Employee's control which is Employer's property.

18. Harassment. Employee acknowledges that Employer has a zero tolerance policy for any form of discrimination or sexual harassment or a hostile work environment. Any breach of this policy by Employee is grounds for immediate dismissal. All complaints of discrimination or sexual harassment should be made to Ryan Bracken or, if you prefer, to counsel for Employer, Anthony G. Barone at (630) 472-0037.

19. Notices. All notices required or permitted under this Agreement shall be in writing and shall be deemed delivered when delivered in person or deposited in the United States mail, postage paid, addressed as follows:

Employer:

Carlton Technologies, Inc.
2000 W. Fulton Street
Chicago, Illinois 60612

Employee:

Jeff Grafstein

Such addresses may be changed from time to time by either party by providing them notice in the manner set forth above.

20. Entire Agreement. This Agreement contains the entire agreement of the parties and there are no other promises or conditions in any other agreement whether oral or written. This Agreement supersedes any prior written or oral agreements between the parties.

21. Amendment. This Agreement may be modified or amended, if the amendment is made in writing and is signed by both parties.

22. Severability. If any provision of this Agreement shall be held to be invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable. If a court finds that any provision of this Agreement is invalid or unenforceable, but that by limiting such provision it would become valid or enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

23. Waiver of Contractual Right. The failure of either party to enforce any provision of this Agreement shall not be construed as a waiver or limitation of that party's right to subsequently enforce and compel strict compliance with every provision of this Agreement.

24. Applicable Law. This Agreement shall be governed by the laws of the State of Illinois.

Employer:

Carlton Technologies, Inc.

By: _____

Ryan Bracken, President

Date: 2/21/02

Agreed to and accepted by:

Employee:

Date: 2-1-02

EXHIBIT 3

BIZ120 INC.
Laser Focused

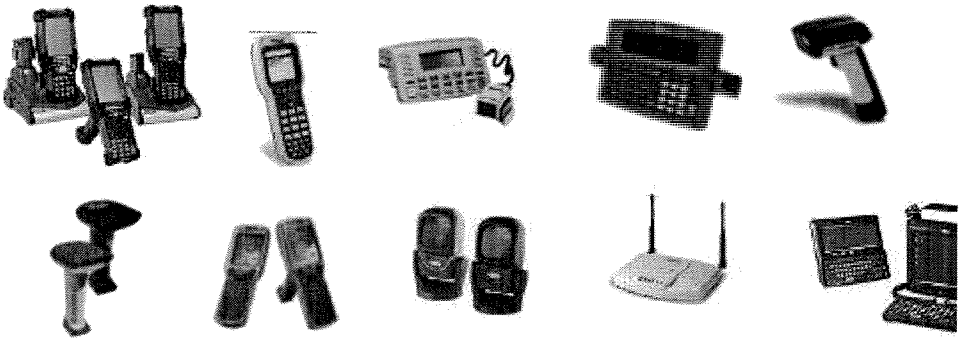
BIZ1 LASER FOC

Under construction!

Thank you for visiting www.biz120inc.com.

Biz 120 provides hardware and repair solutions for scanning and mobile RF devices made by:

- Symbol
- Intermec
- PSC
- HHP
- LXE
- Teklogix
- Zebra



Visit us again soon to learn more about the scanning and wireless products and services that offer.

Contact us:

Phone: 847-831-5149
Fax: 847-831-5169
E-mail: inquiries@biz120inc.com

symbol The Enterprise Mobility Company
psc
LX
HandHeld PRODUCTS
TEKL information in
Zebra
Honeywell BATTERIES Trust your battery
wave
Intermec
MOTORC PartnerSelect Authorized Reseller

EXHIBIT B

EMPLOYMENT AGREEMENT

This Employment Agreement ("Agreement") is entered into as of February 21st, 2002 by and between Carlton Technologies, Inc. ("the Employer"), 2000 W. Fulton Street, Chicago, Illinois 60612, and Jeff Grafstein ("the Employee").

A. Employer is engaged in the business of purchasing, reconditioning and selling product scanners, cash registers and similar devices used at the point of sale in the retail industry and performing services such as refurbishing equipment for others; and

B. Employer has invested a substantial amount of time and resources in developing its business and marketing techniques and in obtaining and maintaining its client and referral base and Employer desires to protect its confidential information and confidential programs and its client base; and

C. Employer desires to retain the services of the Employee and for Employee to assist Employer in developing and maintaining its client base and its business; and

D. Employee is willing to be employed by Employer.

Therefore, the parties agree as follows:

1. **Employment.** Employer shall employ Employee as a Sr. Account Executive and Director of Wireless Data Collection and Scanning Devices. Employee's duties are set forth on Exhibit "A". Employee accepts and agrees to such employment, subject to the general supervision, advice and direction of Employer and the Employer's supervisory personnel. Employee shall also perform such other duties Employer requests Employee to perform. Employee shall also follow all rules of Employer.

2. **At Will Employment.** Your employment with Employer is entered into voluntarily, and you are free to terminate your employment at any time, with or without a reason. Similarly, the Employer has the right to terminate your employment at any time, with or without a reason. Although the Employer may choose to terminate your employment for cause, cause is not required. This is called "at-will" employment. While it is expected that our working relationship will be mutually satisfactory, neither you, nor the Employer, have entered into any express or implied contract of employment for any specified period of time. No one other than the President of the Company that employs you can enter into an agreement for employment for a specified period of time, or make any agreement or representation contrary to the at-will employment policy. The Employer's policy of at-will employment can be changed only in a writing signed by the President of the Company that employs you.

3. **Best Efforts of Employee.** Employee agrees to perform faithfully, industriously, and to the best of Employee's ability, experience, and talents, all of the duties that may be required by the express and implicit terms of this Agreement, to the reasonable satisfaction of Employer. Such duties shall be provided at such place(s) as the needs, business, or opportunities of the Employer may require from time to time.

4. **Compensation of Employee.** As compensation for the services provided by Employee under this Agreement, Employer will pay Employee such compensation as reflected on Exhibit "A". Payments will be made at such payment cycles as the Employer shall determine. Upon termination of this Agreement, payments under this paragraph shall cease, provided, however, that the Employee shall be entitled to payments for periods or partial periods of work that occurred prior to the date of termination and for which the Employee has not yet been paid. Accrued vacation time will be paid in accordance with state law and the Employer's customary procedures.

5. **Absence from Work and Tardiness.** Employer understands that family emergencies and sickness occur which may occasionally require that Employee miss work. In such an event, it is expected that

Employee provide Employer with as much notice as possible of an absence due to an emergency or sickness. Employer may require, in Employer's sole discretion, a note from a physician to verify an illness. Regular full-time employees are entitled to five (5) sick days with pay per year. Sick days are not vacation days and are only to be utilized in the event of a family emergency or an illness which renders Employee incapable of attending work. Sick days may not be carried over from one year to another and Employee is not entitled to receive any pay for unused sick days. Unexcused or excessive absences are grounds for immediate dismissal. Each Employee has a start time. Employee is expected to be at work and ready to begin working at his/her customary start time. Excessive tardiness is grounds for immediate dismissal.

6. **Reimbursement for Expenses in Accordance with Employer Policy.** The Employer will only reimburse Employee for approved out-of-pocket expenses in accordance with Employer policies in effect from time to time.

7. **Recommendations for Improving Operations.** Employee shall provide Employer with all information, suggestions, and recommendations regarding Employer's business, of which Employee has knowledge, that will be of benefit to Employer.

8. **Confidentiality.** Employee recognizes that Employer has and will have information regarding the following:

- products
- margins
- discounts
- business affairs
- marketing plans
- prices
- costs
- future plans
- costs
- customer lists

and other vital information (collectively "Confidential Information") which is valuable, special and unique assets of Employer. Employee agrees that the Employee will not at any time or in any manner, either directly or indirectly, divulge, disclose, or communicate in any manner any Confidential Information to any third party even if such Confidential Information was developed by the Employee during the term of employment of Employee or obtained during or after the term of employment of Employee, without the prior written consent of the Employer. Employee will protect the information and treat it as strictly confidential. A violation by Employee of this paragraph shall be a material violation of this Agreement and, in the event of a violation, Employer shall be entitled to both legal and equitable relief. Employee acknowledges and agrees that the sale or unauthorized use or disclosure by Employee of any Confidential Information of the Employer constitutes unfair competition, and during the term of his employment with the Employer and thereafter, Employee will not engage in any unfair competition with the Employer by directly or indirectly using the Confidential Information, nor will Employee directly or indirectly disclose, publish or make use of, nor authorize anyone else to use Confidential Information or any information or knowledge which in any way relates to the business, product or services of the Employer.

9. **Other Employees.** Employee agrees for a period of two (2) years after the end of his/her employment with the Employer that Employee will not solicit for Employee's benefit or for the benefit of another business or enterprise any person employed by the Employer within six (6) months of Employee's last date of employment.

10. **Non-Solicitation.** In order to protect Employer's longstanding business relationships, Employee agrees that he/she will not, for a period of one hundred and eighty days (180) after his/her employment with Employer ceases for any reason, solicit, directly or indirectly, whether for Employee or as an officer, director, employee, agent or independent contractor of another, for purposes of performing any services or furnishing any equipment of a type similar to that provided by Employer to any client of Employer for whom Employee had contact with during the term of Employee's employment or any person or entity that Employee learned about or obtained any information concerning said person or entity's need for equipment or services as a result of Employee's employment.

"Client," as used herein, shall mean any person or entity for whom Employer performed services or sold equipment within a twelve (12) month period prior to the termination of employee's employment.

11. **Injunction.** Employee agrees that should he/she breach any provision of this Agreement, Employer will suffer irreparable injury and will have no adequate remedy at law. In such an event, Employer shall be entitled to obtain temporary, preliminary and permanent injunctive relief, without bond in any proper court which shall include the Circuit Courts of Cook County, Illinois. In addition to the above, should Employee breach this Agreement, Employer's rights shall be cumulative and Employer may also seek recovery of money damages as well. Thus, all covenants of this Agreement shall survive the termination of Employee's employment.

12. **Records Belong to Employer.** All books, records, files, forms, reports, accounts, papers and documents relating in any manner to the Employer's business, vendors, suppliers, or customers, whether prepared by Employee or anyone else, are the exclusive property of the Employer and shall be returned immediately to the Employer upon termination of employment or upon the Employer's request at any time. This excludes items that belonged to the Employee prior to beginning his/her employment with Employer.

13. **Employee's Inability to Contract for Employer.** Employee shall not have the right to make any contracts or commitments for or on behalf of Employer without first obtaining the express written consent of Employer.

14. **Vacation.** The Employer provides vacation time for Regular Full-Time employees and expects employees to take time away from work to renew their energy and enjoy some leisure activities with family or friends. The amount of vacation time is reflected on Exhibit "A". You may not receive pay in lieu of vacation, except as required by law upon termination of your employment or as Employer shall agree. In order to insure that Employer is sufficiently staffed to continue orderly operations, vacation time must be pre-approved at least two weeks in advance. Employer may, in its sole discretion, not approve a request for vacation time due to scheduling problems or other business demands.

15. **Holidays.** Employee shall be entitled to the following holidays with pay during each calendar year:

- New Year's Day
- Independence Day
- Thanksgiving Day
- Memorial Day
- Labor Day
- Christmas Day

16. **Compliance With Employer's Rules.** Employee agrees to comply with all of the rules and regulations of Employer.

17. **Return of Property.** Upon termination of employment, the Employee shall deliver all property (including keys, records, notes, data, memoranda, models, and equipment) that is in the Employee's possession or under the Employee's control which is Employer's property.

18. **Harassment.** Employee acknowledges that Employer has a zero tolerance policy for any form of discrimination or sexual harassment or a hostile work environment. Any breach of this policy by Employee is grounds for immediate dismissal. All complaints of discrimination or sexual harassment should be made to Ryan Bracken or, if you prefer, to counsel for Employer, Anthony G. Barone at (630) 472-0037.

19. **Notices.** All notices required or permitted under this Agreement shall be in writing and shall be deemed delivered when delivered in person or deposited in the United States mail, postage paid, addressed as follows:

Employer:

Carlton Technologies, Inc.
2000 W. Fulton Street
Chicago, Illinois 60612

Employee:

Jeff Grafstein

Such addresses may be changed from time to time by either party by providing them notice in the manner set forth above.

20. Entire Agreement. This Agreement contains the entire agreement of the parties and there are no other promises or conditions in any other agreement whether oral or written. This Agreement supersedes any prior written or oral agreements between the parties.

21. Amendment. This Agreement may be modified or amended, if the amendment is made in writing and is signed by both parties.

22. Severability. If any provision of this Agreement shall be held to be invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable. If a court finds that any provision of this Agreement is invalid or unenforceable, but that by limiting such provision it would become valid or enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

23. Waiver of Contractual Right. The failure of either party to enforce any provision of this Agreement shall not be construed as a waiver or limitation of that party's right to subsequently enforce and compel strict compliance with every provision of this Agreement.

24. Applicable Law. This Agreement shall be governed by the laws of the State of Illinois.

Employer:

Carlton Technologies, Inc.

By: _____

Ryan Bracken, President

Date: 2/21/02

Agreed to and accepted by:

Employee:

Date: 2-1-02

EXHIBIT C

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

07 C 6757

CARLTON TECHNOLOGIES, INC.,

Plaintiff,

v.

JEFFREY GRAFSTEIN and BIZ 120, INC.,

Defendants.

Case No. 07 _____

Trial by Jury Demanded

JUDGE COAR
MAGISTRATE JUDGE MASON

COMPLAINT FOR INJUNCTIVE AND OTHER RELIEF

Plaintiff, Carlton Technologies, Inc. ("Carlton"), by its attorneys, and for its Complaint for Injunctive and Other Relief against Jeffrey Grafstein ("Grafstein") and Biz 120, Inc. ("Biz 120"), states as follows:

Nature of the Case

1. This is an action to obtain relief for, *inter alia*, violation of the federal Computer Fraud and Abuse Act by Carlton's former employee, Grafstein; Grafstein's blatant violations of the confidentiality and non-solicitation provisions in his Employment Agreement with Carlton; misappropriation of Carlton's trade secrets in violation of the Illinois Trade Secrets Act; and breach of fiduciary duty by Grafstein. While still employed as a trusted, highly-compensated employee of Carlton, where he had access to Carlton's confidential and proprietary information, Grafstein formed a company, Biz 120, to directly compete with and intentionally divert business opportunities away from Carlton using Carlton's own trade secrets and confidential information. Although Carlton's investigation into Grafstein's activities is ongoing, it is evident thus far that Grafstein: (a) accessed Carlton's computer systems for the purpose of stealing numerous files and records containing Carlton's confidential information and trade secrets about its customers,

business practices, pricing strategies, and techniques, which he is now using to compete unfairly with Carlton on a daily basis; (b) intentionally diverted business opportunities from Carlton while still under its employment; and (c) solicited and engaged in business transactions with Carlton customers during the restricted non-solicitation period under the Employment Agreement. Unless enjoined by the Court, Grafstein and Biz 120 will continue to violate Carlton's contractual, statutory, and common law rights, cause irreparable injury to Carlton's business, and continue to compete unfairly with Carlton.

The Parties

2. Carlton is an Illinois corporation with its principal place of business located at 939 North Avenue, Suite 640, Chicago, Illinois.

3. Grafstein is an individual residing at 729 Sumac Road, Highland Park, Illinois.

4. Biz 120 is an Illinois corporation with its principal place of business in Highland Park, Illinois. On information and belief, Grafstein is the sole owner and employee of Biz 120.

Jurisdiction

5. Jurisdiction is proper pursuant to 28 U.S.C. § 1331 and 28 U.S.C. § 1367. Count I alleges a violation of the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* This Court has supplemental jurisdiction over the remaining claims because they "are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy." 28 U.S.C. § 1367(a).

Venue

6. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because, *inter alia,* Grafstein resides in this judicial district, Biz 120 maintains an office in this judicial district, and Grafstein's and Biz 120's unlawful conduct occurred in this judicial district.

The Business of Carlton

7. Formed in 1998, Carlton is a leader in providing and servicing refurbished wireless data collection devices, bar code scanners, and related hardware for commercial clients throughout the United States, Canada, and Europe.

8. Carlton has devoted significant time and expense to developing its confidential customer list. Carlton has three sales professionals who are devoted full-time to developing new business opportunities and servicing existing customers.

9. Carlton's relationships with its customers are recurring and long-term in nature. Carlton has been doing business with the majority of its customers for several years.

10. At great time and expense, Carlton has compiled a database of critical confidential information about its customers and prospective customers that provides it with a competitive advantage. Information within this database includes key contacts and decision makers; historical purchase information for each customer; a communication log identifying each communication with the customer reflecting their past, present, and future purchasing, selling, and maintenance needs; pricing strategies; profitability; gross and net profit margins; specific customer installation platforms detailing all equipment and accessories they used in the past and present; and each customer's plans for future purchases and maintenance. This information is not available publicly.

11. Carlton also buys refurbished and new products from outside vendors. Carlton maintains confidential information about the various vendors, including what products they currently or typically have in inventory, when they may be making these products available, the pricing strategies, profitability, and gross and net profit margins for past transactions. This information is confidential.

12. In its computer systems, Carlton maintains numerous files titled "electronic price ordering guides" or "epog's." This information contains various confidential information about specific products, including part numbers, part descriptions, list prices, and distribution prices. Carlton has compiled these epog files over the course of many years. These files are invaluable to Carlton as this information is no longer publicly available.

13. Carlton has implemented several strict security measures to insure that its confidential information and trade secrets are not used or disclosed outside of Carlton or outside of the key employees with whom such information is shared. For example, all Carlton computer systems are password protected with access limited to employees on a need-to-know basis. In addition, all employees of Carlton are required to sign confidentiality agreements in which they acknowledge the confidential nature of Carlton's information, agree not to use or disclose such information to the detriment of Carlton, and agree to return all such information to Carlton at the conclusion of their employment. The cabinets, desks, and office areas where documents reflecting Carlton's confidential information are retained are not open to persons who are not employed by Carlton.

Grafstein's Employment with Carlton

14. Carlton hired Grafstein as Senior Account Executive and Director of Wireless Data Collection and Scanning Devices commencing on February 21, 2002. In connection with his hiring, Grafstein entered into an Employment Agreement with Carlton (the "Employment Agreement"). A true and correct copy of the Employment Agreement is attached hereto as Exhibit A.

15. The Employment Agreement provides, in relevant part:

8. Confidentiality.

Employee recognizes that Employer has and will have information regarding the following:

- products
- margins
- discounts
- business affairs
- marketing plans
- prices
- costs
- future plans
- costs
- customer lists

and other vital information (collectively "Confidential Information") which is valuable, special and unique assets of Employer. Employee agrees that the Employee will not at any time or in any manner, either directly or indirectly, divulge, disclose, or communicate in any manner any Confidential Information to any third party even if such Confidential Information was developed by the Employee during the term of employment of Employee or obtained during or after the term of employment of Employee, without the prior written consent of the Employer. Employee will protect the information and treat it as strictly confidential. A violation by Employee of this paragraph shall be a material violation of this Agreement and, in the event of a violation, Employer shall be entitled to both legal and equitable relief. Employee acknowledges and agrees that the sale or unauthorized use or disclosure by Employee of any Confidential Information of the Employer constitutes unfair competition, and during the term of his employment with the Employer and thereafter, Employee will not engage in any unfair competition with the Employer by directly or indirectly using the Confidential Information, nor will Employee directly or indirectly disclose, publish, or make use of, nor authorize anyone else to use Confidential Information or any information or knowledge which in any way relates to the business, product or services of the Employer.

* * *

10. Non-Solicitation.

In order to protect Employer's longstanding business relationships, Employee agrees that he/she will not, for a period of one hundred eighty days (180) after his/her employment with Employer ceases

for any reason, solicit, directly or indirectly, whether for Employee or as an officer, director, employee, agent or independent contractor of another, for purposes of performing any services or furnishing any equipment of a type similar to that provided by Employer to any client of Employer for whom Employee had contact with during the term of Employee's employment or any person or entity that Employee learned about or obtained any information concerning said person or entity's need for equipment or services as a result of Employee's employment. "Client," as used herein, shall mean any person or entity for whom Employer performed services or sold equipment within a twelve (12) month period prior to the termination of employee's employment.

11. Injunction.

Employee agrees that should he/she breach any provision of this Agreement, Employer will suffer irreparable injury and will have no adequate remedy at law. In such an event, Employer shall be entitled to obtain temporary, preliminary and permanent injunctive relief, without bond in any proper court which shall include the Circuit Courts of Cook County, Illinois. In addition to the above, should Employee breach this Agreement, Employer's rights shall be cumulative and Employer may also seek recovery of money damages as well. Thus, all covenants of this Agreement shall survive the termination of Employee's employment.

12. Records Belong to Employer.

All books, records, files, forms, reports, accounts, papers and documents relating in any manner to the Employer's business, vendors, suppliers, or customers, whether prepared by Employee or anyone else, are the exclusive property of the Employer and shall be returned immediately to the Employer upon termination of employment or upon the Employer's request at any time. This excludes items that belonged to the Employee prior to the beginning his/her employment with Employer.

13. Return of Property.

Upon termination of employment, the Employee shall deliver all property (including keys, records, notes, data, memoranda, models, and equipment) that is in the Employee's possession or under the Employee's control with is Employer's property.

16. As a Senior Account Executive, Grafstein's responsibilities included establishing and maintaining relationships with a large number of Carlton's customers. Grafstein had regular

contact with those customers, and he had access to confidential information concerning pricing, revenues, budgets, forecasts, and customer contact information about all of Carlton's customers.

17. Grafstein created proposals for customers and pitched the proposals to the customers. Grafstein also met with clients on a regular basis and participated in phone conversations to establish and maintain good customer relationships. Grafstein attended sales meetings at Carlton where the sales team would discuss new customers, new pitches, and any other important issues. In his position, Grafstein had access to all of Carlton's computer systems and confidential files.

18. Grafstein did not bring an established set of revenue generating customers with him when he joined Carlton. A majority of the accounts assigned to Grafstein were introduced to him by Carlton.

19. During the course of his employment with Carlton, Grafstein had access to Carlton's most confidential information and trade secrets, as described above.

20. Grafstein resigned from his employment with Carlton on February 8, 2007.

Grafstein's Formation of Biz 120 to Unfairly Compete With Carlton

21. Unbeknownst to Carlton, Grafstein surreptitiously began planning his exit from Carlton well before February 2007. According to public records, Grafstein incorporated Biz 120 in the State of Illinois in December 2006. In December 2006, Grafstein also purchased a domain name and created his website, biz120inc.com.

22. Biz 120's business model is indistinguishable from Carlton's business model. Biz 120 actively buys, sells, and repairs a broad range of technology in direct competition with Carlton. Biz 120 buys various products, including hand held scanners, imagers, and wireless data collection terminals and sells reconditioned scanners and other accessories. Biz 120 also

repairs scanners and other wireless devices. Biz 120's website, www.biz120inc.com, promotes itself as providing the identical services Carlton provides (e.g., "Biz 120 provides hardware and repair solutions for scanning and mobile RF devices").

23. In or around late December 2006, while still employed by Carlton, Grafstein created Biz 120 to directly compete against Carlton. Also during that time, Grafstein intentionally diverted business leads and opportunities from Carlton to Biz 120. While Carlton's investigation is still ongoing, Carlton's preliminary investigation has revealed at least two business opportunities Grafstein did not reveal to Carlton. Both transactions requested quotes for specific products and services that Grafstein deliberately neglected to enter into Carlton's system.

Breaches of Employment Agreement and Other Unlawful Conduct by Grafstein

24. Carlton recently discovered that, on a single day in October 2006, Grafstein accessed hundreds of files in Carlton's computer systems containing Carlton's confidential information. These files include:

- Business Plan Outline—contains confidential information regarding Carlton's business model and specific business plan.
- E-D Order and Receipt Procedure—contains confidential information about Carlton's fifth largest customer including its order history as well as preferred procedures for orders, including quantities and pricing information.
- E-D Repair Procedures—contains confidential information regarding Carlton's fifth largest customer and details the processes and procedures for servicing and repairing its specific products.
- Epog—contains product pricing, product part numbers, product descriptions, and quantity information that is no longer available to the public.
- gm-by-prod—contains Carlton's confidential gross profit margin information by product.
- Goals—contains Carlton's confidential business goals.
- Maintenance 2005—contains confidential information regarding Carlton's service and repairs for its second largest service customer, including what products it repaired, cost

information, and legal requirements. Grafstein had no legitimate business reason to access this information, the contract was not up for renewal at that time.

- Purchase Contract-AccuCode—contains confidential information regarding customer purchases, including legal requirements on each contract, pricing, and quantity information.

- Repair Procedures—contains confidential information that Carlton has compiled regarding the repair of its products as well as legal requirements for each.

25. Carlton's investigation has revealed that, in connection with his enigmatic plan, Grafstein improperly attached a portable media device to Carlton's company issued laptop and downloaded confidential Carlton documents to this external media source for no legitimate business reason with the intent to directly compete and divert business opportunities from Carlton. For example, Grafstein downloaded a "Price Guide." This document, labeled confidential, contains confidential product and pricing information, including list price, distributor price, and Carlton's sales price for multiple products, which would enable Grafstein and Biz 120 to under bid Carlton on all future business opportunities and transactions. Grafstein also downloaded four documents titled "Epog 95," "Epog 97," "Epog 98," and "Epog 99," which further allow Grafstein and Biz 120 to directly and unfairly compete against Carlton on a daily basis.

26. Grafstein is able to use this confidential information for the benefit of himself and Biz 120. The use of all of the sensitive and confidential information Grafstein misappropriated during his employment and prior to his resignation from Carlton allows Grafstein to underbid and divert business opportunities from Carlton and unfairly compete with Carlton utilizing its confidential information.

27. The files that Grafstein accessed are invaluable to an individual starting a competing company, such as Biz 120. They provide Grafstein and Biz 120 with an unfair

competitive advantage with respect to product pricing strategies, customer specific pricing strategies, and customer specific requirements, to name a few.

28. Although the non-solicitation period in the Employment Agreement did not expire until August, Grafstein blatantly ignored this restriction, solicited Carlton's customers, and diverted business opportunities from Carlton on behalf of Biz 120. One example of Grafstein's violation of the non-solicitation agreement occurred on May 25, 2007. Grafstein sent an email to the main purchasing contact of a long-time customer of Carlton using the identical font, format, and content of a document he took from Carlton. The email promoted Biz 120 as an active buyer, seller, and repairer of a broad range of technology including hand held scanners and wireless data collection terminals. Grafstein had contact with this individual during the term of his employment, and Carlton performed services or sold equipment to this customer within a twelve (12) month period prior to the termination of his employment. Grafstein knowingly violated the terms of his Employment Agreement. On information and belief, Grafstein sent multiple identical or similar communications to other Carlton customers and contacts during the restricted period.

29. During the restricted period, Grafstein also went further than just contacting a Carlton customer. Grafstein and Biz 120 sold and shipped products to Carlton's second largest customer. Grafstein and Biz 120 utilized the confidential pricing and product information that Grafstein stole from Carlton to gain a competitive advantage and directly divert business opportunities from Carlton. Grafstein knew he was to have no contact with this customer and intentionally violated his Agreement with Carlton.

30. Grafstein and Biz 120 are directly competing with Carlton in the exact areas in which Carlton has developed its competitive edge. Grafstein and Biz 120 have an unfair

competitive advantage against Carlton because Grafstein can use his knowledge of confidential information about Carlton's pricing and revenue information, customer information, and marketing plans, to steal current and prospective customers and contacts from Carlton.

31. On information and belief, Grafstein and Biz 120 retained and are currently using records containing Carlton's confidential information and trade secrets.

32. Grafstein not only accessed a number of Carlton files containing confidential information from his work computer and his home computer, but he intentionally attached a portable media storage system to steal files from Carlton's computer system for personal gain. No legitimate business justification existed for Grafstein to access such files at that time. Grafstein accessed files relating to confidential business plans, confidential customer pricing information, confidential sales forecasts, and revenue forecasts.

COUNT I

(Violation of the Computer Fraud and Abuse Act by Grafstein)

33. Carlton realleges and restates paragraphs 1 - 32 as if fully restated herein.

34. The Computer Fraud and Abuse Act provides for a private right of action against anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved an interstate or foreign communication." 18 U.S.C. §§ 1030(a)(2)(C).

35. Carlton has maintained and at all relevant times maintained a computer network that is used to communicate with and service customers throughout the United States, Canada, and Europe. Carlton's computer system is connected to multiple offices, including in Illinois, Michigan, and Canada, and Carlton maintains an interstate computer network. Carlton's computer network is used in interstate and foreign commerce.

36. In the months leading up to Grafstein's resignation, Grafstein accessed Carlton's computer system on multiple occasions to obtain Carlton's confidential and trade secret information for purposes of unfairly competing against Carlton.

37. Grafstein transferred documents, files, and information copied or taken from Carlton's computer network.

38. By dishonest means, Grafstein knowingly and with the intent to defraud accessed Carlton's computer network for its confidential information and, by means of unauthorized access, Grafstein furthered the intended fraud and obtained confidential information of value.

39. Each instance of Grafstein's accessing and obtaining information without authorization constitutes a separate violation of the Computer Fraud and Abuse Act. Carlton has been damaged as a result thereof by the amount of at least $5,000 in the past year, including in the form of, *inter alia,* payments for measures aimed at discovering the extent and consequences of Grafstein's unauthorized activities and damage to the integrity of the data.

COUNT II

(Violation of Illinois Trade Secrets Act by Grafstein and Biz 120)

40. Carlton realleges and restates paragraphs 1 - 39 as if fully restated herein.

41. As set forth above, Grafstein was given access to and is in the possession of certain confidential and proprietary information of Carlton constituting "Trade Secrets" as defined in the Illinois Trade Secrets Act ("ITSA"), 765 Ill. Comp. Stat. 1065/1 *et seq.*

42. Carlton's customer lists, historical purchase information, pricing strategies, profitability, gross and net profit margins, and equipment needs and plans are sufficiently secret

to derive economic value from not being generally known to other persons or entities who can obtain economic value from its use or disclosure.

43. Carlton's customer lists, historical purchase information, pricing strategies, profitability, gross and net profit margins, and equipment needs and plans are the subject of efforts that are reasonable under the circumstances to maintain their secrecy or confidentiality.

44. Grafstein and Biz 120 have used, disclosed or threatened to use or disclose Carlton's trade secret information with full knowledge that this information was acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use.

45. Grafstein and Biz 120's unauthorized use or disclosure, actual or threatened, violates the Illinois Trade Secrets Act, 765 ILCS 1065/1, *et seq.*

46. Grafstein and Biz 120's misappropriation, use, and disclosure of Carlton's trade secrets will cause irreparable harm for which there is no adequate remedy at law. As a result of the foregoing, Carlton has suffered and will continue to suffer irreparable harm.

Count III

(Breach of Contract by Grafstein)

47. Carlton realleges and restates paragraphs 1 - 47 as if fully restated herein.

48. The Employment Agreement is a valid and enforceable contract.

49. Carlton fully performed all of its obligations under the Employment Agreement.

50. Grafstein has breached the Employment Agreement by, *inter alia*, (a) soliciting customers whom he was prohibited from soliciting during the restricted period; and (b) misappropriating and utilizing Carlton's confidential information.

51. Unless an injunction is issued prohibiting Grafstein from utilizing Carlton's confidential information, Carlton will suffer irreparable and incalculable harm, including the

continued loss of proprietary and confidential information for which it may never be compensated.

COUNT IV

(Breach of Fiduciary Duty by Grafstein)

52. Carlton realleges and restates paragraphs 1 - 52 as if fully restated herein.

53. Grafstein, as an employee of Carlton, owed fiduciary duties with respect to the conduct of Carlton's business. These fiduciary duties included the obligation to deal honestly, loyally, fairly and openly with Carlton and to not usurp business opportunities.

54. Grafstein breached his fiduciary duties to Carlton by, *inter alia,* (a) failing to devote his entire time, energy, attention and loyalty to the business of Carlton; (b) competing with Carlton through his improper use of Carlton's proprietary and confidential information; (c) soliciting actual and prospective Carlton customers and diverting Carlton's business to Biz 120 while still employed by Carlton.

55. By reason of the foregoing, Grafstein and Biz 120 have directly and proximately caused injury to Carlton, and Carlton has suffered, and continues to suffer, substantial injury as a result of Grafstein's breaches of his fiduciary duties.

PRAYER FOR RELIEF

Wherefore, Carlton requests that judgment be granted in its favor and against Grafstein and Biz 120 and that it be granted:

(a) A preliminary and permanent injunction order barring Grafstein, Biz 120, his agents, and any third party acting in concert with him from using, copying, analyzing or disseminating Carlton's confidential, proprietary information in any fashion;

(b) An order granting Carlton's representatives immediate access to Grafstein's residence to take possession of: (1) any and all documents, files, or any other materials which are the property of Carlton; (2) any and all computers belonging to or under the control of Grafstein; and (3) any and all computer storage media, including floppy disks, CD-ROMS, CD-Rs, CD-Read/Write discs, optical discs, flash memory, USB drives, disks, or memory, Zip disks, Jazz disks, Superdisks, removable or portable hard disks, removable or portable electronic storage and/or any other computer storage media under Grafstein's control which may contain files and/or any other electronic information constituting the property of Carlton, and/or which may contain, comprise, include and/or incorporate trade secrets and/or confidential information belonging to Carlton;

(c) A permanent injunction against Grafstein, Biz 120, their agents, and any person acting in concert with them, prohibiting them from using or disclosing Carlton's confidential proprietary and/or trade secret information;

(d) An order directing Grafstein, Biz 120, their agents, and any person acting in concert with them, to account for and return to Carlton any and all documents containing or reflecting information concerning Carlton's customers, products, or business, in whatever form, including electronic files, that Grafstein and/or Biz 120 retained following the resignation of Grafstein's employment with Carlton;

(e) disgorgement of profits unlawfully obtained by Grafstein and Biz 120;

(f) return of the compensation paid to Grafstein during the period of disloyalty;

(g) compensatory and punitive damages;

(h) attorney's fees and costs; and

(i) such other and further relief as may be appropriate.

Respectfully submitted,

CARLTON TECHNOLOGIES, INC.

By: /s/ John M. Dickman

John M. Dickman
Ronald Y. Rothstein
Sheila P. Frederick
WINSTON & STRAWN LLP
35 West Wacker Drive
Chicago, Illinois
(312) 558-5600
(312) 558-5700 (fax)

Attorneys for Plaintiff

EXHIBIT D

Slip Copy, 2007 WL 2377335 (N.D.Ill.)

(Cite as: 2007 WL 2377335 (N.D.Ill.))

H

Only the Westlaw citation is currently available.

United States District Court,
N.D. Illinois,
Eastern Division.
AMERICAN FAMILY MUTUAL INSURANCE, COMPANY, Plaintiff,
v.
Bonnie L. ROTH, d/b/a Bonnie Roth Agency, Connie S. Roth, d/b/a Connie Roth Agency, and Roth and Roth Insurance Agency, Inc., d/b/a Roth and Roth Insurance, Defendant.
No. 05 C 3839.

Aug. 16, 2007.

James P. Denardo, Kristin Dvorsky Tauras, Sarah A. Cook, McKenna, Storer, Rowe, White & Farrug, Chicago, IL, for Plaintiff.

Michael Joseph Daley, Anthony Packard, Nisen & Elliott, Chicago, IL, Wallace C. Doolittle, Law Office of Wallace C. Doolittle, Hayward, CA, William P. Tedards, Jr., Washington, DC, for Defendants.

REPORT AND RECOMMENDATION RE: PLAINTIFF'S MOTION FOR RULE TO SHOW CAUSE

JEFFREY COLE, Magistrate Judge.

I.
BACKGROUND

***1** On June 30, 2005, American Family Mutual Insurance Company ("AFM" or "plaintiff"), filed a five-count complaint seeking preliminary and permanent injunctive relief, pursuant to Rule 65, Federal Rules of Civil Procedure, against Bonnie L. Roth, d/b/a Bonnie Roth Agency, Connie S. Roth, d/b/a Connie Roth Agency, and Roth and Roth Insurance Agency, Inc., d/b/a Roth and Roth Insurance, (collectively, "the defendants"). The complaint charged that the defendants misappropriated certain confidential information from AFM's confidential, policyholder files in violation of the Wisconsin Trade Secrets Act (Count I), used and disclosed that information in violation of the Gramm Leach Bliley Act ("GLBA" or "the Act"), 15 U.S.C. § 6801 *et. seq.* (Count II), breached their Agent Agreements with AFM by soliciting at least two AFM policyholder to purchase insurance through the defendants (Count III), tortiously interfered with AFM's contracts with its policyholders, who were solicited (Count IV), and tortiously interfered with AFM's prospective business expectations (Count V).

On July 14, 2005, Judge Guzman granted AFM's motion for a temporary restraining order, which prohibited the defendants from:

> personally or through any person, agency, company or organization directly or indirectly inducing or attempting to induce or assisting anyone else in inducing or attempting to induce any Roth Policy holders (as defined below) of the American Family Companies to lapse, cancel, replace or surrender any insurance policy in force with American Family Life Insurance Companies. "Roth Policyholder" means any policyholder credited to the account of Bonnie and Connie Roth at the time of the termination with American Family Insurance on February 15, 2005. [FN1]
>
> FN1. Accounts credited to the Roths consisted of active policies, but excluded inactive policies and prospects. *See Opposition to AFM's Motion For A Rule to Show Cause* at 4-10.

The TRO ran for ten days and was extended by Judge Guzman for an additional ten days. Pursuant to Judge Guzman's referral, I conducted a preliminary injunction hearing on August 2 and 3,

2005, and met with counsel on August 4. On August 5, 2005, I issued my Report and Recommendation, which recommended that a preliminary injunction be issued against the defendants' use of any information downloaded from AFM's database. This included approximately 1,700 pages of confidential customer related information.

The proof at the preliminary injunction hearing showed that in May 2005 the Roths sent a mass emailing to "their American Family customers," announcing their new independent insurance business. (*Opposition To Motion For Rule To Show Cause* at 11). The email letter (Exhibit 34) was sent to 1,847 individuals. The evidence at the hearing led to the firm conclusion the likely source of the names was AFM's database, and that the Roths' claim that they had purchased the names from an outside vendor was mendacious. *See American Family Mutual Ins. Co. v. Roth,* 2005 WL 3700232 at *4, 15-16 (N.D.Ill.2005). [FN2] Post-hearing discovery also confirmed what the hearing proof showed, namely that the Roths had also misappropriated lists of their active policyholders without the knowledge of AFM and in contravention of the agreements with it. (*See Exhibits* 7, 35; *Opposition To AFM's Motion For Rule To Show Cause* at 14).

> FN2. Exhibit 34 also consisted of a 38-page list of the email addresses and names of the 1,847 people to whom the email was sent. *See American Family Mutual Ins. Co. v. Roth,* 2006 WL 2192004 at *4 (N.D.Ill.2006) (Guzman, J.). The 1,847 names included the active policyholders assigned to the Roths' accounts, inactive policyholders, and screened prospects. The Roths claim that there were 1,050 clients they serviced ignored the latter two components. *Id.*

***2** On August 3, 2005, the defendants through counsel, agreed in open court to continue to abide by the terms of the TRO, until Judge Guzman ruled on the matter. AFM was "perfectly comfortable" with that agreement. (*Plaintiff's Motion for Rule to Show Cause,* Ex. A, 8/3/2005 Transcript, at 457).

In an exhaustive Memorandum Opinion and Order dated July 27, 2006, Judge Guzman concluded that the "likely source" of the 1,847 names listed in Exhibit 34 was AFM's database, that the names in the Email Concept database utilized by the Roths constituted a list of AFM customers and qualified for trade secret protection, and that the Roths had misappropriated the information--actually, that the Roths had waived any argument that they had not misappropriated it. In fact, Judge Guzman's analysis demonstrated that based on a representative sampling, 90% of names in Exhibit 34 also appeared in the AFM database. *See American Family Mutual Ins. Co. v. Roth,* 2006 WL 2192004 at *5 (N.D.Ill.2006). Judge Guzman granted AFM's motion and ordered it to provide a proposed preliminary injunction order. On August 10, 2006, Judge Guzman entered a Preliminary Injunction under which the defendants were:

1. ... enjoined from using for any reason any information downloaded from [AFM's] database, including the names contained in Exhibit 34.
2. ... enjoined from servicing [AFM] customers,
3. ... required to disclose to [AFM] the [AFM] customers contacted since February 11, 2005, and the customers who have responded to the solicitation,
4. ... required to return to [AFM] all materials in their possession related to [AFM] customers, and
5. ... required to preserve the status quo.

(Dkt # 67). The defendants filed a notice of appeal of this order on September 8, 2006.

While the appeal was pending, AFM filed the instant "Motion for Rule to Show Cause," arguing that the defendants should be held in contempt for violating the TRO that was extended by agreement until Judge Guzman entered the Preliminary Injunction, as well as for having violated the Preliminary Injunction itself. The motion charges the defendant with various violations, which can be categorized as: (1) emailing customers, (2) retaining AFM materials, and (3) failing to disclose customer contacts. The offending emails--which are the focus of AFM's motion--were sent on the following dates, among others: August 17, 2005; January 31, 2006; February 23, 2006; February 28, 2006; April 12, 2006; May 15, 2006; and May 28, 2006. (*Plaintiff's*

Motion For Rule to Show Cause, at 8-10; *Opposition to Motion For A Rule To Show Cause* at 15). AFM has not made the emails a part of the record, and only their topics are adverted to. Four of the emails (including those sent on August 17, 2005, and May 15, 2006) dealt with auto insurance, which the Roths have conceded AFM active policyholders might have had. (*Opposition to Motion For Rule To Show Cause* at 15). Two, including the February 28, 2006 email, dealt with homeowners insurance, which the Roths also concede was a type of insurance which the AFM active policyholders might have had. (*Motion For Rule To Show Cause* at 15).

***3** The email of February 23, 2006 was apparently an article on Chicago highway speedtraps. The others were greeting cards--for Ground Hog Day, Easter, and Memorial Day. (*Plaintiff's Motion for Rule to Show Cause,* at 9-10; Ex. F). Beyond a finding of contempt, AFM asks that Bonnie Roth be required to produce her laptop for forensic examination to ensure that all lists of AFM customers are permanently deleted; that the defendants be required to give AFM access to their commercial database to ensure that all customers of AFM are deleted; and for an award of attorneys fees.

On May 7, 2007, the Seventh Circuit agreed that AFM was entitled to a preliminary injunction because the customer information stolen by the Roths from AFM's database constituted a trade secret. *American Family Mut. Ins. Co. v. Roth,* 485 F.3d 930 (7th Cir.2007). Judge Posner concluded that it was "highly likely, though not certain" that most of the 1,847 names in Exhibit 34 were names of customers in the group of 2,000 customers that the plaintiff had assigned to the defendants during the course of their agency relationship with the plaintiff. *Id.* at 932. Of course, "[n]othing in the legal process is certain, *United States v. Chaidez,* 919 F.2d 1193, 1200 (7th Cir.1990), and not even the stringent burden of proof beyond a reasonable doubt requires certainty. *See Branion v. Gramly,* 855 F.2d 1256 (7th Cir.1988).

While affirming Judge Guzman's granting of the preliminary injunction, the Court of Appeals was troubled by some of its wording, especially "the inclusion in the prohibition against downloading of 'the names contained in Exhibit 34.' " *Id.* at 934. The court explained that, "[w]hile most of the names are in the database, some are not, and there isn't any basis for forbidding the defendants to use those names." *Id.* The court also indicated that the provision regarding " 'servicing' the plaintiff's customers" should probably be stricken. *Id.* Accordingly, it remanded the case "for the entry of a better-drafted injunction." *Id.*

A month later, the Preliminary Injunction was amended. It enjoined the defendants from:

1. using for any reason any information downloaded from or obtained in any way from [AFM]'s database, including the names contained in Exhibit 34 which are also in [AFM]'s database;
2. soliciting [AFM]'s customers who were assigned to either defendant's accounts on February 15, 2005;
3. are required to disclose to [AFM] the [AFM] customers contacted since February 11, 2005 and the customers who have responded to the solicitation;
4. are required to return to [AFM] all materials in their possession related to [AFM] customers; and
5. Are required to preserve the status quo.

II.
ANALYSIS
A.
Law Applicable to Contempt Proceedings

" 'A court's civil contempt power rests in its inherent limited authority to enforce compliance with court orders and ensure judicial proceedings are conducted in an orderly manner.' " *United States v. Dowell,* 257 F.3d 694, 699 (7th Cir.2001). To be held in civil contempt, a person must have violated an order or decree that sets forth in specific detail an unequivocal command. *Id.* at 699. It is not necessary to a finding of contempt that a violation was "willful." It is enough that a party "has not been reasonably diligent and energetic in attempting to accomplish what was ordered." *Goluba v. School Dist. of Ripon,* 45 F.3d 1035, 1037 (7th Cir.1995).

***4** The party asserting a violation of a judicial

order has the burden of proving the violation by clear and convincing evidence--which is, of course, a greater burden of proof than preponderance of the evidence. *Maynard v. Nygren,* 332 F.3d 462, 469 (7th Cir.2003); *Dowell,* 257 F.3d at 699; *Hernandez v. O'Malley,* 98 F.3d 293, 295 (7th Cir.1996). The Supreme Court has defined it as placing "in the ultimate fact-finder an abiding conviction that the truth of ... [his] factual contentions are 'highly probable' " *Colorado v. New Mexico,* 467 U.S. 310, 316, 104 S.Ct. 2433, 81 L.Ed.2d 247 (1984). *See also United States v. Boos,* 329 F.3d 907, 911 (7th Cir.2003); *von Gonten v. Research Systems Corp.,* 739 F.2d 1264, 1268 (7th Cir.1984). [FN3]

> FN3. In other contexts, the standard has been variously defined as evidence: (1) "that produce[s] in the mind of the trier of fact a firm belief or conviction as to the truth of the allegations sought to be established, evidence so clear, direct and weighty and convincing as to enable [the factfinder] to come to a clear conviction, without hesitancy, of the truth of the precise facts in issue," *Cruzan by Cruzan v. Director, Missouri Dept. of Health,* 497 U.S. 261, 285, 110 S.Ct. 2841, 111 L.Ed.2d 224 (1990); (2) "sufficient to 'enable the [trier of fact] to come to a clear conviction, without hesitancy, of the truth of the precise facts in issue.... It is not necessary that the evidence be uncontradicted.. provided it 'carries conviction to the mind' or carries 'a clear conviction of its truth'...," *United States v. Askari,* 2007 WL 1073698, *4 (3rd Cir.2007); or (3) "which leaves no reasonable doubt in the mind of the trier of fact as to the truth of the proposition in question." *Parker for Lamon v. Sullivan,* 891 F.2d 185, 188 (7th Cir.1989). Despite its word choice, the latter formulation cannot be read to conflate the standards of proof beyond a reasonable doubt with proof by clear and convincing evidence.

The function of any standard of proof is to indicate the degree of confidence society thinks a factfinder should have in the correctness of factual conclusions for a particular type of adjudication. By informing the factfinder in this manner, the standard of proof allocates the risk of erroneous judgment between the litigants and indicates the relative importance society attaches to the ultimate decision. *Colorado,* 467 U.S. at 315-16. The requirement in cases of contempt that the evidence be clear and convincing manifests society's judgment that the risk of error is to be borne by the party seeking the contempt order and its unwillingness to allow punishment for a claimed violation of a court order, save where the evidence warrants a high degree of confidence in the correctness of the determination that a contempt has occurred. *See Autotech Technologies Ltd. Partnership v. Automationdirect.Com, Inc.,* 2006 WL 1304949, *4 (N.D.Ill.2006) (collecting cases).

B.

The TRO And The Preliminary Injunction

At the outset, it is important to distinguish between the prohibitions of the TRO and those of the Preliminary Injunction. In AFM's view, throughout this case, the defendants have been under some sort of general order that was an amalgam of the TRO, the Report and Recommendation, and the Preliminary Injunction. But the requirements and prohibitions of the TRO and the Preliminary Injunction are very different, and the Report and Recommendation had no preclusive effect. Once Judge Guzman had ruled on it, it was his Preliminary Injunction, not the Report and Recommendation, that was the operative order.

A temporary restraining order cannot remain in force for more than 20 days without the consent of the parties. *Chicago United Industries, Ltd. v. City of Chicago,* 445 F.3d 940, 942 (7th Cir.2006); *United States v. Board of Educ. of City of Chicago,* 11 F.3d 668, 671 (7th Cir.1993); Rule 65(b), Federal Rules of Civil Procedure. The parties, of course, are free to consent to have the TRO extended beyond the 20-day period. Such agreements are common. *See, e.g., Planned Parenthood v. Attorney General,* 297 F.3d 253, 258 (3d Cir.2002); *Tenafly Eruv Ass'n, Inc. v. Borough of Tenafly,* 309 F.3d 144, 154-155 (3rd Cir.2002);

Geneva Assur. Syndicate, Inc. v. Medical Emergency Svcs. Associates (Mesa), 964 F.2d 599 (7th Cir.1992); *Ruiz v. Commissioner of Dept. of Transp. of City of New York,* 858 F.2d 898, 901 (2nd Cir.1988). But if the order is extended by the court without consent, it automatically becomes a preliminary injunction, regardless of what the district court calls it. *See United Airlines, Inc. v. U.S. Bank N.A.,* 406 F.3d 918, 923 (7th Cir.2005); *In re Criminal Contempt Proceedings Against Gerald Crawford,* 329 F.3d 131, 136 (2d Cir.2003).

***5** Judge Guzman extended the TRO for an additional 10 days. On August 3, 2005 the parties agreed to abide by the TRO until Judge Guzman ruled on AFM's motion for a preliminary injunction, thereby, in effect, agreeing to an extension of the TRO. [FN4] Contrary to AFM's assertion, this agreement did not convert the TRO to an appealable preliminary injunction. (*Plaintiff's Motion for Rule to Show Cause,* at 7). "An order supported by consent is not appealable," *United Airlines,* 406 F.3d at 923, and a TRO extended by consent beyond 20 days is not a preliminary injunction. *See Geneva,* 964 F.2d at 599(TRO extended by consent remains a "bona fide, true-blue temporary restraining order, and therefore it was not appealable."); *Ross v. Evan,* 325 F.2d 160 (5th Cir.1963) (TRO extended by consent does not lose its character as "a nonappealable TRO and become converted into an appealable preliminary injunction"). [FN5]

> FN4. The defendants' solemn promise--and it was surely that (*Motion for Rule to Show Cause* at 4)--to obey the TRO was no less binding than if Judge Guzman had entered another order with the parties' consent further extending the TRO. *Cf. Tamari v. Bache & Co.,* 729 F.2d 469, 472 (7th Cir.1984) (attorney's promise in open court to produce documents can be treated as the equivalent of an order for Rule 37(b) purposes); *Doi v. Halekulani Corp.,* 276 F.3d 1131, 1138 (9th Cir.2002).
>
> FN5. AFM concludes that statements made in colloquy with the parties near the end of the preliminary injunction hearing signified a ruling that any TRO that extends beyond 20 days becomes a preliminary injunction whether imposed on the parties without their consent by the court or by consent of the parties to extend the TRO beyond the 20 day period. (*Motion for Rule to Cause* at 4, 7). The parties had been referred to Judge Easterbrook's opinion dealing with that issue, and it was that opinion and not an off-hand comment that was operative. *Cf. Geneva,* 964 F.2d at 599 ("but a misapprehension of the rules governing appealability does not convert a temporary restraining order into a preliminary injunction.").
> Moreover, the statement quoted by AFM was followed by this statement: "And I will take you all at your word that this--nothing is going to happen between the time Judge Guzman gets this [Report and Recommendation] and he makes a decision one way or the other." *Id.* Obviously, if the TRO had turned into a preliminary injunction, there would have been no need for any agreement by the parties to abide by the TRO, and it would have been unnecessary to "take [counsel] at [their] word that nothing is going to happen" until Judge Guzman ruled.

Under the terms of the TRO, the defendants were not to attempt to induce any policyholders credited to their accounts at the time of their terminations (i.e. active policyholders) to lapse, cancel, replace, or surrender any insurance policy in force with AFM. While the Report and Recommendation envisioned a preliminary injunction with broader prohibitions than that, it was merely a recommendation until Judge Guzman conducted the *de novo* review mandated by 28 U .S.C. § 636(b)(1) and issued his decision. *See Pinkston v. Madry,* 440 F.3d 879, 894 (7th Cir.2006).

It is beyond debate that my Report and Recommendation had no binding effect since a magistrate judge has no authority to grant injunctive

relief, absent a consent by all parties to jurisdiction. 28 U.S.C. § 636(b)(1)(A); 28 U.S.C. § 636(c)(1). *See also E.E .O.C. v. Local 638,* 81 F.3d 1162, 1182 (2nd Cir.1996); *Alpern v. Lieb,* 38 F.3d 933, 935 (7th Cir.1994). In short, AFM's argument--at least its apparent argument--that the Report and Recommendation constituted some sort of order binding on the defendants or that the Report and Recommendation of its own force either extended or expanded the TRO is mistaken. (*AFM's Reply,* at 2-4). [FN6]

> FN6. AFM likens the situation here to that in *Levine v. Comcoa, Ltd.,* 70 F.3d 119, 1192 (11th Cir.1995), where the district court issued an order from the bench that indefinitely extended a previously entered TRO. Two things distinguish that case from this. Judge Guzman never extended the TRO past the 20 day time period. Second, the order extending the TRO--which the 11th Circuit concluded constituted a preliminary injunction since it was issued without consent--was from an Article III judge and thus was effective, *ex proprio vigore.* The only question there was what was the effect of the extension. Here, I had no authority to issue any sort of injunctive relief, and a report and recommendation from a magistrate judge, has no independent operative effect. *Cf.* 28 U.S.C. § 636(b)(1).

Thus, in order to establish contempt regarding the emails sent by the defendants at any time in the period from July 14, 2005--when the TRO was issued--until August 10, 2006, when Judge Guzman entered the preliminary injunction, AFM must demonstrate by clear and convincing evidence that the defendants attempted to induce AFM active policyholders credited to the Roths' accounts to cancel their policies or allow them to lapse. As to any post-August 10 conduct, AFM must prove that the defendants violated the Preliminary Injunction or Amended Preliminary Injunction entered on June 6, 2007.

AFM's motion focuses on the defendants' use of the 1,847 names in Exhibit 34 in repeated emailings in the period August 2005 to August 2006. But the use of the list, *simpliciter,* is not a violation of the TRO. Exhibit 34 was not mentioned in the TRO, although it was a salient feature of the Report and Recommendation and the Preliminary Injunction. (*Plaintiff's Motion for Rule to Show Cause,* at 7-13). Since, however, the Report and Recommendation had no preclusive or binding effect, the claim that the defendants used the list of 1,847 names "for at least 13 mailings from between August 5, 2005 and August 10, 2006" to solicit AFM customers, is not dispositive. (*Plaintiff's Motion for Rule to Show Cause,* at 7-9). [FN7]

> FN7. Between August 5, 2005 and August 2006, the Roths sent 19 emailings utilizing the Email Concept Database containing the information on Exhibit 34. Six of these emailings were sent to more than 2,000 individuals. The numbers ranged from 2,213 to 2,333 recipients. (*See Motion For Rule To Show Cause,* Ex. F). The designations on Exhibit F reflected that the emailings were for "homeowners insurance," "speed traps on Chicago freeways," "e-offer auto mailer," "auto insurance." *Id.*

***6** Suppose for example, that the Roths were convinced that Judge Guzman would refuse to enter a preliminary injunction and in anticipation utilized Exhibit 34 to prepare a mailing to AFM customers soliciting their business and urging them to cancel their present policies. The defendants planned to send the emails the moment the anticipated favorable ruling issued. That use of Exhibit 34 would not violate the TRO so long as the inducing solicitations were never sent. Thus, to make its case, AFM must prove that there was a prohibited mailing to a prohibited recipient. The first inquiry deals with the content of the email, the second with the identity of the recipient. [FN8]

> FN8. At another point, AFM takes a different tack, arguing that Exhibit 34 was a protected trade secret and that "whether restrained by the injunction or counsel's

agreement, or simply by the law of trade secrets, the [defendants] were not at liberty to continue unfettered use of Exhibit 34." (*Plaintiff's Motion for Rule to Show Cause,* at 8). But in *this* motion, AFM is seeking have the defendants held in contempt for violating a court order and, consequently, it must be able to point to an order or decree that sets forth in specific detail an unequivocal command. *Dowell,* 257 F.3d at 699. As such, this proceeding is not a vehicle to enforce, generally, trade secret law; *see In re Debs,* 158 U.S. 564, 596, 15 S.Ct. 900, 39 L.Ed. 1092, (1895) ("[A] court, enforcing obedience to its orders by proceedings for contempt, is not executing the criminal laws of the land, but only securing to suitors the rights which it has adjudged them entitled to."); or an agreement between parties. *Tranzact Technologies, Inc. v. ISource Worldsite,* 406 F.3d 851, 855 (7th Cir.2005) (settlement agreement not enforceable through contempt proceeding when its terms are not expressly set forth in court order); *John Maye Co., Inc. v. Nordson Corp.,* 753 F.Supp. 1451, 1457 (E.D.Wis.1990) (restraining order could not be orally modified). Rule 65(d) requires an order describing in reasonable detail the acts to be restrained, and not merely reference some other document or agreement. *Blue Cross and Blue Shield v. American Express Co.,* 467 F.3d 634, 636 (7th Cir.2006). Here, the only such order was the TRO, at least until Judge Guzman entered the Preliminary Injunction.

C.

AFM's Evidence Regarding The Emails

Until Judge Guzman entered the Preliminary Injunction on August 10, 2006, the defendants were prohibited (by virtue of their agreement to abide by the TRO) from attempting to induce any AFM active policyholders credited to the Roths' accounts at AFM as of February 15, 2005, "to lapse, cancel, replace or surrender any insurance policy in force with [AFM]."

The easiest part of the proof, it would seem, would be in proving that emails went to credited policyholders, which could be accomplished simply by matching the names of the recipients with the names of AFM's customers credited to the defendants at the time of the severance of their relationship with AFM. AFM has not done this and the Roths claim that it is impossible to determine whether an email went to a prohibited person except by extrapolation since the use record at Email Concepts "does not record the individual recipients by name." (*Opposition To Motion For A Rule To Show Cause* at 15). Wherever the truth may lie, the only obvious fact is that the parties' presentations on this score are labyrinthine and, as presented, somewhat inconclusive. It is also obvious that the Roths insisted they did everything possible to comply with the TRO while at the same time denying any knowledge of the TRO's continuing prohibitions after August 5th. (*Motion For Rule To Show Cause* Ex. B, Dep. of Bonnie Roth at 57). [FN9]

FN9. Ms. Roth claims that she was never told that she was under an injunction.

1.

The Deposition Testimony Of Bonnie Roth

It is AFM's contention that Bonnie Roth's (purported) admission that the defendants contacted "active policyholders" between August 5, 2005 and August 10, 2006, by using Exhibit 34, is sufficient to find that the defendants guilty of contempt.

As Judge Posner noted, the "vast majority" of the 1,847 names on the list of names included in Exhibit 34 "were also in the plaintiff's database," and that "it is highly likely, though not certain, that most of those were names of customers in the group of 2,000 customers that the plaintiff had assigned to the defendants" *American Family,* 485 F.3d at 932. The defendants insist, however, that only 380 people in the Email Concept system were active policyholders at the time of termination. (*Opposition To Motion For A Rule To Show Cause* at 14). We need not resolve the issue, for the defendants accept this figure for purposes of its motion, and, more importantly, Ms. Roth conceded

at her deposition that she contacted "active policyholders." (*See Plaintiff's Motion for Rule to Show Cause,* at 7-8).

*7 Ms. Roth contended that she and her sister were adding new leads to the 1,847 names in Exhibit 34, although she could not say with precision exactly how many or when. AFM's own proof showed that the defendants were adding prospects to the database. (*Plaintiff's Motion for Rule to Show Cause,* Ex. B, at 85-86; *Id.* at Ex.F; *Id.* at Ex. K; *Defendants' Opposition,* Ex. 4). Exhibit F reflects a mailing on 1/29/05 to 2,050 individuals. The mailing was a Happy Ground Hogs Day card. On 5/22/05, the Roths sent out an announcement of their new business venture to 1,847 individuals (Ex. 34), the very likely source of which was AFM's database of active accounts, inactive accounts and screened prospects.

Bonnie Roth admitted that as of February 15, 2006, when the contractual one year solicitation period lapsed, *American Family,* 2005 WL 3700232 at * 3, she felt she could, and in fact probably did, contact active policyholders of AFM. (*Plaintiff's Motion for Rule to Show Cause,* at 8; Ex. B at 98-100). But the permissibility of the solicitations was a function of the TRO, not the non-compete. Given Ms. Roth's view of the case, there would have been no reason for her to have exercised any restraint regarding permissible mailings, and she obviously did not do so, notwithstanding the TRO which defined what the Roths could and could not do. Thus, she has in effect admitted that the mass mailings between February 15, 2006 and August 5, 2006--if they constituted inducements-- violated the TRO.

Further proof that the emailings prior to the issuance of the Preliminary Injunction went to AFM active customers is provided by a comparison of the emailings before and after August 10, 2006. Exhibit F reveals numerous mailings to in excess of 2,000 recipients per emailing between the Report and Recommendation and August 2006 when the Preliminary Injunction was issued. Thereafter, there was a precipitous decline in email traffic. For example, of the 12 emailings in that period, the largest number was to 652 people. The next largest was to 346, 343, and 340 people respectively. The remaining emailings are much smaller. Next to each mailing appears the phrase, "new leads." Thus, the evidence demonstrates that following the Preliminary Injunction there was an immediate cessation of large mass emailings to a group that obviously included active AFM policyholders. This is persuasive evidence of the defendants' prior knowledge and intent of the restrictions of the TRO at the time of the earlier mass mailings. *Cf.* Rule 404(b), Federal Rules of Evidence; *United States v. Chavis,* 429 F.3d 662, 669 (7th Cir.2005) (subsequent acts admissible to show prior knowledge and intent). *Compare Hemsworth v. Quotesmith.com, Inc.,* 476 F.3d 487, 491 (7th Cir.2007) (suspicious timing of an event can constitute persuasive circumstantial evidence).

Having said this, the *particular testimony AFM cites* does not support its characterization of Bonnie Roth's testimony:

> ***8** Q: And in all of those other e-mails that went out, where the e-mails are in excess of 2000, what assumption, do you make any assumptions about those?
> A: I would make an assumption based on the time period.
>
> * * *
>
> The Groundhogs Day, that probably went to, I would assume that probably most of the categories prospects and inactives, the actives and any other categories I had at the time which was--
> Q: What's the date of that one?
> A: The date of this one is 1/29/05. And it probably would have went to the membership listing, the category I have for the membership listing, Chamber of Congress that wasn't part of Exhibit 34.

(*Plaintiff's Motion for Rule to Show Cause,* Ex. B, at 81-82). Since the email under discussion was sent in January of 2005, nearly six months before AFM filed suit, AFM's argument regarding this purported admission is unavailing.

Finally, at another point in its motion, AFM relies on this same exchange to assert that Ms. Roth admitted that *every* emailing with more than 2,000

recipients went to "active customers." But the question focused on one email that was sent before this litigation. In addition, plaintiff's counsel posed another question to Ms. Roth before she could finish her statement about "the actives." When she was allowed to continue, Ms. Roth made it clear that the particular email under discussion, which was not subject to the TRO, went to individuals who were not part of Exhibit 34.

2.

The Mathematical Proof

The second aspect of AFM's proof of contempt is mathematical. For example, AFM notes that:

> Prior to February 15, 2006, the die date for the non-solicitation clause, *it appears* the Roths contacted active policyholders.... In a document submitted as part of their response to Am Fam discovery requests, *it appears* that no new names were submitted to the data base until September of 2006, that document also shows that up until that time, the Roths solicited the names on Exhibit 34....The size of the Email Concepts Database at the time the Roths left Am Fam *appears* to exceed 2000 names, but Exhibit 34 of 1847 names has always been the number used.

(*Plaintiff's Motion for Rule to Show Cause,* 8-9 (emphasis supplied)). The tentative phrasing of the argument seems inconsistent with the contention that the proof is clear and convincing. Rather, the phrasing is closer to a "more likely than not" test. But an order issued on such terms is not an order based on clear and convincing evidence. *See Maynard,* 332 F.3d at 469 (characterizing ruling based on what "was more likely than not" and circumstantial evidence as failing to meet the "clear and convincing evidence" standard).

Mr. Robert Krumroy, who founded the internet marketing data company (Email Concepts) to which the defendants subscribe, testified that when using his company's email system, a client could categorize a customer list by certain types of information. He gave the example of entering into the database whether customers were Christians or Jews, which would allow the system to target the appropriate holiday greeting card for each. (*Plaintiff's Motion for Rule to Show Cause,* Ex. H, at 22). Mr. Krumroy testified that one could either send emails to an entire database, or to one category--but not to combinations of categories. (*Plaintiff's Motion for Rule to Show Cause,* Ex. H, at 23). [FN10] Mr. Krumroy was emphatic that "it would not be a logical assumption" that merely because a mailing went to more than 2,000 people it must have gone to the entire database. (*Motion for Rule to Show Cause,* Ex. H, at 23).

> FN10. Not surprisingly, Ms. Roth's deposition testimony--or at least parts of it--were at odds with Mr. Krumroy's. She claimed that some of her emailings, she could not say which ones, only targeted certain categories, which ones she could not say. (Deposition of April 3rd at 36).

***9** AFM's math is convoluted and rests on certain assumptions that do not appear to be correct, the most significant one being that no names were added to the Email Concepts database from the time the Roths left AFM until September 2006. But Exhibit F shows mailings in excess of 2,000 before September 2006. However, one need not resolve the debate about the legitimacy of the assumptions on which AFM's argument is based and which are disputed vigorously by the defendants.

The January 31, 2006 mailing went to 2,133 people. Bonnie Roth claimed not to know whether this included active policyholders. (*Motion For Rule To Show Causes,* Ex. B, Deposition of April 3rd at 31). As to the February 2006 email to 2,222 people, she said that based on the number of emails sent, "it probably would have gone out to, yes, the entire database." *Id.* at 30. She based that testimony on her knowledge of the number of leads and new leads acquired since she and her sister were terminated by AMF. *Id.* But if that be true, the earlier emailing also must have gone to the entire database as well, for included within the database were the 1,847 names, which in turn were comprised of "active policyholders," inactive policyholders and screened prospects. Thus, it is of no moment whether the real number of active policyholders was 380 or any other number. The same is then true of the additional emails in April

and May 2006 that went to over 2,300 recipients. Since there were at least 380 people who were concededly active policyholders in the Email Concepts database, (*Opposition To Motion For A Rule To Show Cause* at 14), the above emailings must have included these people. [FN11]

> FN11. AFM disputes the accuracy of the 380 number but oddly makes no attempt to refute it although it would appear to be simplicity itself for AFM to disprove the number. It seems odd that despite the passage of two years from the date of the Preliminary Injunction hearing, AFM has yet to prove how many of the 1,847 names in Exhibit 34 were credited policyholders at the time the Roths' relationship with AFM was terminated.

3.
AFM Has Failed To Demonstrate By Clear And Convincing Evidence That The Emails Violated The TRO's Prohibition Against "Inducing" The Recipients To Cancel Their Insurance With AMF

This brings us to the second aspect of the proof necessary for a finding of contempt, namely whether the emails, themselves, constituted inducements to the recipient to "to lapse, cancel, replace or surrender any insurance policy in force with [AFM]." The emails are not attached as exhibits, and there are only the laconic descriptions in Exhibit F such as "Group Health," "Indexed Annuities," "Auto Insurance," "Happy Groundhog Day," "Homeowners Insurance," "Roth IRA," "E-cards: Easter Greeting Card; E-cards: Memorial Day Card." Nor is there any meaningful discussion of or argument regarding the content of the purportedly offending emails or argument as to why they qualify as attempted inducements. (*Motion For Rule To Show Cause* at 10)

These sorts of descriptions are not sufficiently informative to be able to conclude that there is clear and convincing evidence that the corresponding emails sought to induce the recipients to cause them to cancel their policies with AFM or to allow them to lapse or to do any of the other things the TRO prohibited. Calling something an inducement does not make it so any more than calling a building personalty makes it personal property. *In re TCI Ltd.*, 769 F.2d 441 (7th Cir.1985). [FN12]

> FN12. Mr. Krumroy testified that working from a database of names and information provided by his clients, Email Concept's system can send out targeted emails automatically. The emails might be financial newsletters and related information, or they might just be holiday, birthday, or anniversary greetings. (*Motion for Rule to Show Cause,* Ex. H, Krumroy Dep. at 7, 21-22).

***10** Just as every idea is an incitement, *Gitlow v. New York,* 268 U.S. 652, 673, 45 S.Ct. 625, 69 L.Ed. 1138 (1925) (Holmes, J., dissenting), every contact by the Roths to a prospective customer might cause the recipient to look favorably on them and ultimately to change from AFM to the Roths by allowing their policies to lapse or by canceling them. But that would not qualify as an inducement any more than the expression of an idea qualifies as an incitement to prohibited action. AFM deals with the issue simply by presupposing that the emailings qualify as prohibited inducements. [FN13] This sort of non-presentation is insufficient to sustain the burden of proof by clear and convincing evidence that the defendants sent inducements to members of the prohibited class.

> FN13. Financial information might qualify as an inducement to drop AFM insurance coverage although, in the past, plaintiff's counsel has not been so sure. (*See* Report and Recommendation, at 32). An email about auto insurance or homeowners insurance would more likely qualify. But not necessarily. A simple holiday greeting--such as an Easter card--qualifies is certainly not as clear. An email providing some financial news and mentioning a product would be one thing; an email that says, "Happy Ground Hog Day," would be another.

D.

The Defendants' Retention of AFM Materials

The injunction required the defendants "to return to [AFM] all materials in their possession related to [AFM] customers...." The Amended Preliminary Injunction Order did not alter this requirement. The defendants argued at the preliminary injunction hearing that with one exception, they had either returned or destroyed the hundreds and hundreds of pages of customer information surreptitiously taken from AFM. The Roths' former lawyers assured the court that they had advised their clients of the need to continue to abide by the TRO. (*See Transcript citations* at *Motion For Rule To Show Cause* at 4). [FN14] It is undisputed that the Roths knew of the TRO and of their need not to violate it in the period following the preliminary injunction hearing and before Judge Guzman acted on the Report and Recommendation. (*See Motion For Rule To Show Cause,* Ex. J at 48. *See also* Ex. b at 86).

FN14. As noted earlier, Bonnie Roth, not surprisingly, denied it.

The August 5, 2005 Report and Recommendation explained at length the basis for my credibility determinations and why I found incredible the Roths' testimony regarding the claimed shredding of hundreds of pages of "personal insurance reviews and account summaries," which were replete with personal policyholder information, including personal health information, prior contacts, validity of drivers licenses, employment information, including job title and duties, policy rates and numbers, effective dates of policies and renewals. The Report and Recommendation came to the same conclusion regarding Connie Roth's testimony that she did not know why she downloaded the 244 pages of active and inactive prospects. (*AFM's Trial Exhibit* 7). She said she didn't need them and repeated that she did not know why she did it. Not surprisingly, there was no explanation of why she would have retained these documents, while *purportedly* shredding the infinitely more informative, several hundred pages of personal insurance reviews for all *her* customers.

All-in-all, the evidence was overwhelming that the Roths had downloaded or copied from AFM's databases some 1,700 pages of AFM customer-related information that they had used and not returned even though obligated to do so by their contract with AFM, and that they lied about having returned or destroyed all those documents. Thus, the Report and Recommendation stated that I was "unable to and d[id] not accept the Roths' testimony that all the materials they downloaded are no longer in their possession"--except for the customer list in Exhibit 34. The Report and Recommendation concluded that "the Roths' testimony was disingenuous and designed to conceal their retention of copies of all or substantially all of the information misappropriated from AFM." *American Family,* 2005 WL 3700232, at *15-17. [FN15]

FN15. I also found incredible the Roths' claim that Exhibit 34 was merely a list of prospects, the overwhelming majority of which they had developed through purchases of lists from outside vendors. *Id .,* at *15. That finding was adopted by Judge Guzman and was undisturbed by the Court of Appeals.

***11** Judge Guzman's *de novo* review of my determinations led him to agree that much of the Roths' testimony was "incredible," and he "adopt[ed my] findings as to their credibility." *American Family,* 2006 WL 2192004, at *3. Judge Guzman found that the kind of "gamesmanship" practiced by the Roths in their testimony, "when taken in the context of the other instances of incredible testimony illustrates the Roths' *general dishonesty* regarding the facts at issue." (Emphasis supplied). He went on to say that "the record is filled with many more specific instances of the defendants giving incredible and disingenuous testimony and the above examples are simply some of the more egregious." Judge Guzman concluded by saying that "the Court finds the Roths' testimony incredible and adopts Magistrate Judge Cole's findings on all credibility issues." *American Family,* 2006 WL 2192004 at *4. [FN16]

FN16. Perjury, as Judge Posner has said, is a fraud on the court. *Allen v. CTA,* 317

> F.3d 697, 703 (7th Cir.2003). It strikes at the heart of the integrity of the judicial system and is incompatible with the values underlying any system of justice. *See United States v. Mandujano,* 564, 425 U.S. 576 (1976); *United States v. Kennedy,* 372 F.3d 686, 695 (4th Cir.2004). *Cf. Escamilla v. Jungwirth,* 426 F.3d 868, 870 (7th Cir.2005) (Easterbrook, J.) ("The legal system offers many ways to deal with problems; perjury is not among them.").

Most significantly, for purposes of the present discussion, Judge Guzman found "it incredible that the Roths would have been deterred by running out of ink and that the testimony on this subject was intended to conceal the fact that they actually have the documents." *Id.* at *4. These credibility determinations were not disturbed by the Court of Appeals. Hence, the inescapable fact is that the Roths lied about the existence of some (if not all) of the 1,700 documents they impermissibly misappropriated from AFM, and then failed to return the documents notwithstanding the clear command of the preliminary injunction.

In light of the findings made by the Report and Recommendation and by Judge Guzman, it is no less true today than it was in August 2006 when Judge Guzman issued a preliminary injunction that the documents continue to exist. It is undisputed that these documents have yet to be returned to AFM. There is absolutely no credible evidence--indeed no evidence at all--that the mass of documents misappropriated by the Roths from AFM were in fact destroyed. The only post-preliminary injunction hearing testimony on this score, and it is of recent origin, relates to Exhibit 34. Ignored is the AFM customer-related material that the evidence demonstrated in 2005 and in 2006 the Roths had in their possession.

On Friday, August 10, 2007, I initiated a conference call with counsel for AFM and for the defendants to determine whether there had ever been any delivery of any document from the defendants to AFM or its counsel. AFM's counsel said that the defendants had never returned any AFM customer-related documents to AFM. The defendants' present counsel, Mr. Tedards, who has been in the case since October 2006, confirmed that he had made no such turnover but would check with prior counsel to see what occurred between August 2005 and October 2006.

On Tuesday, August 14th, I had a further telephone conference call with all counsel, and it was confirmed that there had been no turnover of AFM customer-related materials by prior counsel. Mr. Tedards informed me that Mr. Packard, the defendants' prior counsel, told him that he had in his possession a box of "printouts" of materials. These would appear to be materials downloaded or otherwise taken by the Roths at the time of their separation from AFM. Mr Tedards said that at a deposition on July 28, 2005 Mr. Packard said on the record that he planned to retain "any printouts" until the litigation ended. That box of materials is still in Mr. Packard's possession. Mr. Tedards said that he does not have copies. Mr. Tedards said that the deposition transcript reveals that when Mr. Packard informed AFM's counsel of his intent to retain the documents the response was, "okay."

***12** Whatever the "okay" may have signified in 2005, it was meaningless once the Preliminary Injunction issued with its unambiguous commands--commands which have yet to be obeyed.

The defendants concede that Bonnie Roth had an electronic version of Exhibit 34 on her computer--for use with Email Concepts--until she purportedly deleted it in February or March of 2007. (*Opposition To Motion For A Rule To Show Cause,* at 17). She claimed to have done so not because of some ethical compunction or fidelity to her obligations under the Preliminary Injunction, but because, she said, the database was growing too large and could result in increased costs. AFM argues that her testimony is contradicted by that of Mr. Krumroy and that her testimony was "characteristically obfuscat[ory]." (*Motion For Rule To Show Cause* at 10-11). Exhibit N, which was filed as a separate document in support of the reply [170] is a compendium of what AFM claims are numerous and significant contradictions of

statements made by the Roths in affidavits submitted in opposition to the Motion For Rule To Show Cause. Certain of the examples support the conclusion that the Roths' current affidavit testimony simply cannot be taken at face value.

Even if the Roths' current affidavit testimony is to be credited--a dubious proposition in light of the multiple inconsistencies in the post-August 5, 2005 discovery and in light of their performance at the Preliminary Injunction hearing-- [FN17] it is undisputed that for a period of 6 months following the Preliminary Injunction, they maintained Exhibit 34 on one of their computers. This, itself, is a violation of the Preliminary Injunction. The only rejoinder is the claim that the TRO merely required that the defendants not *use* the materials. (*Defendants' Opposition,* at 17, 23). But the Preliminary Injunction clearly required the return of the materials in addition to prohibiting their use. The evidence is clear and convincing that the defendants violated the Preliminary Injunction by maintaining an electronic version of Exhibit 34 in their database until February of 2007.

> FN17. Prior perjury is a circumstance to be weighed in determining present credibility. *Alan,* 317 F.3d at 703.

I recommend that the court find that Exhibit 34 continues to exist and has not been returned despite the explicit command of the preliminary injunction. In addition, I further recommend that regardless of the determination regarding present existence, the court find that the 6 month period of retention of Exhibit 34 in digital form constitutes contempt of the Preliminary Injunction's requirement that all customer related information be returned to AFM.

At her deposition on February 12, 2007, Bonnie Roth testified that in August 2005, she used Exhibit 35 (which admittedly was a list of her active accounts while at AFM, (*Opposition to Rule To Show Cause* at 14)--and which has not been returned--to identify the different categories of names on Exhibit 34: prospective, active, and inactive clients. (*Plaintiff's Motion for Rule to Show Cause,* Ex. J, at 50-51). She could not say, however, whether once she completed the task, she returned Exhibit 35 to her attorney:

> ***13** Q: Did [counsel] give you a list of [AFM] customers that you had printed off prior to your departure from AFM for use in creating what we have been calling List B?
> A: This was the exhibit that I had printed off of all your active, inactive and prospects.
> Q: And you had printed that up prior to your departure from [AFM]?
> A: Yes.
> Q: And then you gave that to [counsel]?
> A: I turned everything over to [counsel].
> Q: And he gave it back to you?
> A: I'm not sure the timing of the sequence ... So I can't remember if he gave it to me or vice versa....

(*Id.,* at 41).

Ms. Roth claimed she could not remember if the information from the exhibit remained on her computer or if she deleted it. (*Id.,* at 42-43).

In their brief, the defendants maintain that Exhibit 35 was returned to the lawyers and they have offered to demonstrate as much through a selective waiver of the attorney-client privilege. They have also said there is "no evidence whatsoever to suggest that anything" occurred other than the usage of the list to identify active customers in August 2005 so that the Roths would not run afoul of the TRO. (*Defendants' Opposition,* at 23). This *ipse dixit* ignores the Roths' prior and pervasive perjury at the Preliminary Injunction hearing and its continued usage in connection with the mass emailings between August 2005 and August 2006. Moreover, the offer of selective waiver of attorney-client privilege has no meaning and, in any event, would prove nothing. Return of a document would not prove that the Roths had not retained either an actual or digital copy.

It is recommended that the defendants be found in contempt of that portion of the Preliminary Injunction that required them to return all AFM customer-related information, that they be ordered to make available for immediate forensic examination all computers they possess to ensure all AFM customer-related materials have been deleted,

and that the defendants be ordered to allow AFM access to their electronic database for the same reason. Questions of confidentiality can be resolved by appropriate protective orders and/or by retention of outside experts to report to the court and to counsel under appropriate instructions. All these costs, it is recommended, be borne by the defendants. It is further recommended that the forensic examination be sufficiently comprehensive to determine not only whether AFM customer-related information but when any that did exist was deleted.

E.
Defendants' Failure to Disclose Customer Contacts

Finally, AFM argues that the defendants have not complied with that provision of the Preliminary Injunction that required the defendants "to disclose to [AFM] the [AFM] customers contacted since February 11, 2005, and the customers who have responded to the solicitation...." The Amended Preliminary Injunction Order maintains this requirement. According to AFM, the defendants produced: (1) a 700-page list of people the defendants have admitted soliciting, with last names redacted, without designating whether they are active, inactive, or prospective AFM customers, and (2) a list of active policyholders of Bonnie and Connie Roth that was not in alphabetical order. (*Plaintiff's Motion for Rule to Show Cause,* at 13-14).

***14** There is no legitimate justification for having produced a redacted list of solicitees. That is plainly not compliant with the Preliminary Injunction. After all, since they are AFM customers, they are no secret to AFM. The defendants do not argue otherwise (*Opposition To Motion For A Rule To Show Cause,* at 23-24), and they can hardly be heard to say that they lack the capability of identifying any active AFM policyholder, for they now concede having had their own lists of active policyholders. "Exhibit 7 [at the Preliminary Injunction hearing] was Connie's list and Exhibit 35 [at the hearing] was Bonnie's." (*Opposition To AFM's Motion For A Rule To Show Cause* at 14). Indeed, according to the Roths, they used these lists in late August 2005 to determine who were active policyholders, inactive policyholders, and prospects at the time of their termination. *Id.* at 14; 19. Either the documents were returned to prior counsel, who still retains them in his box of "printouts," or the Roths have them in their actual possession. Either way, compliance with this aspect of the Preliminary Injunction was not difficult. The Roths simply chose not to comply.

There is every reason for the Roths to have produced the lists in the abbreviated and uninformative manner they purposely chose. By refusing to provide last names of those whom they contacted, the Roths have made it impossible for AFM to detect prohibited solicitations during the time that the TRO was extended by agreement or in the period following the Preliminary Injunction.

It is recommended that the Roths be ordered to comply immediately with the Preliminary Injunction's requirement of providing names of AFM customers contacted and it is further recommended that the defendants be found in contempt of this provision of the Preliminary Injunction.

CONCLUSION

AFM has asked that the defendants "be ordered to show cause why they should not be found in contempt." (*Reply* at 16). That would be an empty form of relief since the purpose of a rule to show cause is to provide notice to an individual of what must be responded to. Since the Federal Rules of Civil Procedure, the notice is provided by a "notice of motion" under Rule 7(b), which--obviates the necessity for obtaining such a rule. *See SEC v. VTR, Inc.,* 410 F.Supp. 1309, 1313 n. 3 (D.D.C.1975) (and cases cited). *Cf. Schmude v. Sheahan,* 312 F.Supp.2d 1047, 1064 (N.D.Ill.2004). The defendants have had ample notice of the claims against them and have fully responded to AFM's theories, arguments, and supporting evidence. Hence, there is no necessity for directing such a rule, as Chief Justice Marshall observed in *Life & Fire Ins. Co. of N.Y. v. Adams,* 34 U.S. 571, 9 Pet. 571, 9 L.Ed. 233 (1835).

Notwithstanding its title, the Motion is really a

motion to hold the defendants in contempt of the TRO and the Preliminary Injunction . [FN18] For the foregoing reasons, it is recommended that the plaintiff's Motion [# 137; also filed as # 41 in 05-CV-3867] be construed as a Motion To Hold The Defendants In Contempt and that as construed, it be GRANTED in part and DENIED in part. It is further recommended that, to the extent that the court concludes that the defendants are guilty of contempt as recommended above, AFM be awarded all its attorney's fees and costs incurred in the prosecution of the Motion For Rule To Show Cause, including all costs and expenses incurred in connection with any forensic examination of AFM's computers or any electronic database. *Tranzact Technologies,* 406 F.3d at 855.

> FN18. The defendants have not asked for an opportunity to testify in person, and they have had a full opportunity to present their case. Having further proceedings to enable the defendants to re-present their arguments and testimony in person would only enable a court to evaluate the demeanor of the Roths. But there is infinitely more to credibility determinations than demeanor. *See Indiana Metal Products v. NLRB,* 442 F.2d 46 (7th Cir.1971); *Pinpoint Inc. v. Amazon.Com, Inc.,* 347 F.Supp.2d 579, 583 (N.D.Ill.2004) (Posner, J .) (sitting by designation); *Ginsu Products, Inc. v. Dart Industries, Inc.,* 786 F.2d 260, 263 (7th Cir.1986).

***15** It is further recommended that the documents in the defendants' former counsel's possession be immediately turned over to AFM. Finally, it is also respectfully recommended that there be a monetary penalty imposed in an amount the court deems appropriate and based upon the financial resources of the defendants. *See South Suburban Housing Center v. Berry,* 186 F.3d 851, 845 (7th Cir.1999); *Grove Fresh Dist., Inc. v. John Labatt, Ltd.,* 299 F.3d 635, 642 (7th Cir.2002); *United States v. Dowell,* 257 F.3d 694, 699 (7th Cir.2001).

END OF DOCUMENT

Westlaw.

Not Reported in F.Supp.2d Page 1

Not Reported in F.Supp.2d, 2002 WL 31834009 (W.D.La.)

(Cite as: 2002 WL 31834009 (W.D.La.))

C

Only the Westlaw citation is currently available.

United States District Court,
W.D. Louisiana.
US GREENFIBER
v.
Sherrie BROOKS
No. Civ.A. 02-2215.

Oct. 25, 2002.

RULING

JAMES, J.

***1** Plaintiff U.S. GreenFiber ("GreenFiber") brings this suit for injunctive relief and monetary damages against Defendant Sherrie Brooks ("Brooks") for breach of fiduciary duty, conversion, and alleged violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*, the Louisiana Trade Secrets Act, La.Rev.Stat. § 51:1431 *et seq.*, and the Louisiana Uniform Trade Practices and Consumer Protection Law, La.Rev.Stat. § 51:1401 *et seq.*

On October 18, 2002, GreenFiber filed a motion for temporary restraining order and preliminary injunctive relief [Doc. No. 4]. On October 18, 2002, this Court issued a temporary restraining order enjoining Brooks from: (1) using or disclosing any and all of GreenFiber's business and quality control information; (2) soliciting or otherwise contacting current GreenFiber employees through the use of GreenFiber's communications systems, and (3) disclosing information to lawyers or parties who are adverse to GreenFiber in litigation. This Court also directed Brooks to return GreenFiber's property, equipment, documents, and business and quality control records in her possession, custody, or control. Finally, this Court ordered that a hearing on GreenFiber's motion for preliminary injunction be held on October 24, 2002, at 10:00 a.m. A copy of the temporary restraining order and notice of hearing was served on Brooks on October 19, 2002.

A hearing on GreenFiber's motion for a preliminary injunction was held on October 24, 2002, at 10:00 a.m. Brooks failed to appear. After the hearing, Brooks did file a memoranda in opposition to GreenFiber's motion for a preliminary injunction. Having considered the evidence introduced at the hearing and the argument of counsel and Brooks, GreenFiber's motion for a preliminary injunction is GRANTED.

I. FINDINGS OF FACT

The Court finds the following facts to be established:

Brooks is a former employee of GreenFiber. While at GreenFiber, Brooks was employed as a Quality Control Manager and worked out of her home. In this position, Brooks was responsible for overseeing quality control for ten GreenFiber plants located in the states of Arizona, California, Florida, Georgia, Nebraska, North Carolina, Ohio, Texas, and Virginia.

Brooks maintained all quality control records and documents in her home. These materials were kept and maintained by Brooks in her capacity as a manager for GreenFiber. These documents were made available to Brooks solely because of her position as Quality Control Manager. Any and all documents related to Brooks's job which are or which once were located in her home are the property of GreenFiber.

On October 9, 2002, GreenFiber terminated Brooks's employment while she was at the corporate headquarters in Charlotte, North Carolina.

After her termination, Dave Bowman ("Bowman"),

Brooks's direct supervisor, learned from e-mail correspondence that while Brooks was at GreenFiber's headquarters, she copied documents belonging to GreenFiber and took those documents with her when she left. Bowman wrote Brooks on October 14, 2002, stating: "As we told you in the termination interview, all corporate documents including all copies are proprietary assets of GreenFiber and should be returned to us promptly."

***2** In an October 14, 2002, e-mail to Bowman, Brooks refused to return the documents she took from the headquarters. In that e-mail, Brooks threatened to provide confidential information, trade secrets, property, and documents belonging to GreenFiber to an adverse party in a pending civil case. Brooks threatened to disclose, among other things, e-mails, monthly reports, customer complaints, strategic plans, sales reports, and customer pricing lists. Brooks also threatened to provide these same items to competitors of GreenFiber with whom she allegedly had job interviews. Finally, Brooks threatened to use these same items in a personal lawsuit against GreenFiber.

On October 15, 2002, counsel for GreenFiber wrote to Brooks demanding the return of all GreenFiber's property no later than October 16, 2002.

In response to GreenFiber's demand, Brooks returned a computer and related hardware belonging to GreenFiber on October 17, 2002. GreenFiber's IT Consultant, John Zizzi ("Zizzi"), examined the computer on the day it was returned and determined that all documents, e-mail files, and Microsoft Office, including the Outlook e-mail program, had been removed. GreenFiber later sent the computer to a forensic engineer in California to determine whether any of the deleted data could be recovered.

Brooks did not return the other equipment, property, documents, or materials.

Brooks was aware of GreenFiber's procedures to protect its confidential, proprietary, and trade secret information from theft. In addition to password protection, which limits access to the company's computer databases to authorized employees, GreenFiber has a confidentiality policy that sets guidelines for the employees' use and handling of GreenFiber's business information. Each employee is provided with a copy of this policy, and each employee is required to execute the policy as a condition of employment.

Although Brooks did not execute this policy, it is clear from her e-mail that she was aware of this policy. Furthermore, Dennis Barrineau ("Barrineau"), President of GreenFiber, sent an e-mail to employees who had not executed the policy explaining it to them again.

Despite her knowledge of these policies and GreenFiber's demands for return of its property, Brooks continued to engage in unlawful actions. She also engaged in unauthorized access of the company's communications systems to contact other employees, including Bowman, following her termination.

On October 22, 2002, Brooks sent a FedEx package to GreenFiber's counsel in response to the demand to return all confidential information, trade secrets, property, and documents. Although Brooks returned some of the requested items, Brooks admits that she continues to retain documentation regarding GreenFiber's compliance with government standards.

II. CONCLUSIONS OF LAW

The Court makes the following conclusions of law:

Jurisdiction is proper pursuant to 28 U.S.C. § 1331 because GreenFiber has alleged violations of the CFAA. Further, diversity jurisdiction pursuant to 28 U.S.C. § 1332 exists because GreenFiber and Brooks are citizens of different states and the amount in controversy exceeds $75,000.

***3** In determining whether to grant or deny a preliminary injunction, the Court applies a four-part test:

(1) a substantial likelihood that plaintiff will prevail on the merits;

(2) a substantial threat that plaintiff will suffer

> irreparable injury if the injunction is not granted;
> (3) that the threatened injury to plaintiff outweighs the threatened harm the injunction may do to the defendant; and
> (4) that granting the preliminary injunction will not disserve the public interest.

Canal Authority of State of Florida v. Callaway, 489 F.2d 567, 572 (5th Cir.1974). "A preliminary injunction is an extraordinary remedy and should be granted only if the movant has clearly carried the burden of persuasion with respect to all four factors." *Allied Marketing Group, Inc. v. CDL Marketing, Inc.,* 878 F.2d 806, 809 (5th Cir.1989) (citing *Mississippi Power & Light v. United Gas Pipe Line,* 760 F.2d 618, 621 (5th Cir.1985); *Apple Barrel Productions, Inc. v. Beard,* 730 F.2d 384, 389 (5th Cir.1984)). Failure of the movant to establish any one of the four factors defeats the right to injunction. *See Rohoe, Inc. v. Marque,* 902 F.2d 356 (5th Cir.1990). As discussed below, the Court concludes that GreenFiber has sufficiently established all four factors and, therefore, is entitled to injunctive relief.

A. GreenFiber has Proven a Substantial Likelihood that It Will Prevail on the Merits

1. Computer Fraud and Abuse Act

The CFAA makes it a crime for anyone to "intentionally access[ ] a protected computer without authorization, and as a result of such conduct, cause [ ] ... loss to 1 or more persons during any 1-year period ... aggregating at least $5,000 in value ..." 18 U.S.C. § 1030(a)(5)(A)(iii) and (B)(i). The CFAA also provides that "[a]ny person who suffers damage for loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief ." 18 U.S.C. § 1030(g). A "protected computer" includes a computer "which is used in interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B).

In order for GreenFiber to succeed on its claim that Brooks violated the CFAA, it must establish that Brooks intentionally accessed a protected computer, that she did so without authorization or by intentionally exceeding her authorized access, and that she caused GreenFiber a loss of at least $5,000.

The Court finds that GreenFiber is likely to succeed on the merits of its CFAA claim. The computer at issue was used by Brooks to communicate with GreenFiber's offices and customers involved in interstate and foreign commerce. Although Brooks was not authorized to access GreenFiber's communications systems after her termination, Brooks intentionally accessed GreenFiber's internal e-mail system and sent messages to GreenFiber employees. Brooks also removed from the computer assigned to her all documents, e-mail files, and Microsoft Office, including the Outlook e-mail program. Any authority Brooks may have had to access the computer following her termination did not include the authority to remove these documents and programs. Finally, Bowman's affidavit, together with Barrineau's testimony, support GreenFiber's contention that it suffered damages and losses in excess of $5,000.

2. Louisiana Trade Secrets Act

***4** The Louisiana Trade Secrets Act "authorizes injunctive relief against one who is guilty of actually or threatening to misappropriate a trade secret." *Technical, Inc. v. Allpax Products, Inc.,* Civ. A. No. 90-872, 1990 WL 41924, at *9 (E.D.La. March 28, 1990) (citing La.Rev.Stat. § 51:1432). "In addition to or in lieu of injunctive relief, a complainant may recover damages for the actual loss caused by misappropriation. A complainant also may recover for the unjust enrichment caused by misappropriation that is not taken into account in computing damages for actual loss." La.Rev.Stat. § 51:1433. A "trade secret" is defined as:

> information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (a) derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable by proper means by other persons who can obtain economic value from its

disclosure or use, and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

La.Rev.Stat. § 51:1431(4). The term "misappropriation" means:

(a) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(b) disclosure or use of a trade secret of another without express or implied consent by a person who:

(i) used improper means to acquire knowledge of the trade secret; or

(ii) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was:

(aa) derived from or through a person who had utilized improper means to acquire it;

(bb) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(cc) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(iii) before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

La.Rev.Stat. § 51:1431(2).

"The plaintiff bears the burden of proving both the existence of a legally protectable trade secret and the legal basis upon which to predicate relief." *Technical Inc.*, 1990 WL 41924 at *9.

The Court finds that GreenFiber is likely to succeed on the merits of its Louisiana Trade Secrets Act claim. The information and records at issue constitute "trade secrets" under La.Rev.Stat. § 51:1431(4). Brooks is in possession of sensitive quality control and business records including product compliance records, e-mails, monthly reports, customer complaints, strategic plans, sales reports, and customer pricing lists. According to GreenFiber, this information derives independent economic value from not being generally known to and not being readily ascertainable by other persons, including their competitors and parties adverse to them in pending litigation. Further, GreenFiber has taken reasonable efforts to maintain the secrecy of this information by instituting a confidentiality policy and by using password protection to limit access to this information to authorized employees.

*5 Additionally, Brooks misappropriated GreenFiber's trade secrets when, after her termination, she copied and took documents belonging to GreenFiber which she knew to be proprietary and confidential. Brooks has also threatened to: (1) provide confidential information, trade secrets, property, and documents belonging to GreenFiber to an adverse party in a pending civil case; (2) disclose, among other things, e-mails, monthly reports, customer complaints, strategic plans, sales reports, and customer pricing lists; (3) provide these same items to competitors of GreenFiber with whom she allegedly had job interviews; and (4) use these same items in a personal lawsuit against GreenFiber.

Therefore, the Court concludes that GreenFiber has proven a substantial likelihood that it will succeed on the merits of its CFAA and Louisiana Trade Secrets Act claims.

B. GreenFiber has Proven the Remaining Injunction Factors

Having found that GreenFiber has proven a substantial likelihood that it will succeed on the merits, GreenFiber must also sustain its burden on three other factors before the Court will issue an injunction. GreenFiber must prove: (1) that an injunction is necessary to prevent irreparable injury, (2) that the balance of interests favors issuance of an injunction, and (3) that injunctive relief will not undermine or disserve the public interest.

GreenFiber asserts that it will suffer irreparable injury in the absence of an injunction because Brooks will likely use business, customer, pricing, and quality control information for her improper benefit in her prospective lawsuit. Furthermore, Brooks has also threatened to use that information on behalf of a GreenFiber competitor in a $1.7 million lawsuit against GreenFiber and on behalf of

other GreenFiber competitors with whom Brooks intends to obtain employment. The Court finds these reasons sufficient to show irreparable injury.

GreenFiber also argues that the balance of interests favors the issuance of an injunction. The Court agrees. This injunction will enforce and protect the legal rights of GreenFiber while in no way unfairly limiting Brooks's ability to continue working. Brooks can work at any job she chooses, including going to work for one of GreenFiber's competitors. What she cannot do is disclose confidential, proprietary, and trade secret information.

Finally, GreenFiber asserts that an injunction will not undermine or disserve the public interest. Again, the Court agrees. This injunction will serve to protect the private interests that our state and federal laws intend to protect. The Court finds no countervailing public interest in allowing Brooks to violate the law.

Having found a substantial likelihood that GreenFiber will succeed at trial, the Court concludes that GreenFiber will suffer irreparable injury in the absence of an injunction, that the threatened harm to GreenFiber outweighs the harm that Brooks might sustain, and that enjoining her from using or disclosing GreenFiber's trade secrets, proprietary, business, quality control, customer, and pricing information will not disserve the public interest.

III. CONCLUSION

***6** GreenFiber has carried its burden of persuasion by showing that (1) there is a substantial likelihood that it will prevail on the merits, (2) it will suffer irreparable harm if a preliminary injunction is not granted, (3) the threatened injury to it outweighs the threatened harm the injunction may do to Brooks, and (4) granting the preliminary injunction will not disserve the public interest. Accordingly, GreenFiber's request for preliminary injunctive relief is hereby GRANTED.

ORDER

For the reasons set forth in this Court's Ruling:

IT IS HEREBY ORDERED that Plaintiff U.S. GreenFiber's ("GreenFiber") motion for a preliminary injunction [Doc. No. 4] is GRANTED.

IT IS FURTHER ORDERED that Defendant Sherrie Brooks is (1) enjoined from using or disclosing any and all of GreenFiber's business and quality control information; (2) directed to return GreenFiber's property, equipment, documents, and business and quality control records (including all copies thereof and computer records), in her possession, custody or control; (3) enjoined from soliciting or otherwise contacting current GreenFiber employees through use of GreenFiber's communications systems; and (4) enjoined from disclosing information to lawyers or parties who are adverse to GreenFiber in litigation.

Not Reported in F.Supp.2d, 2002 WL 31834009 (W.D.La.)

END OF DOCUMENT

Not Reported in F.Supp.2d

Page 1

Not Reported in F.Supp.2d, 2006 WL 2990432 (N.D.Ill.), 84 U.S.P.Q.2d 1297

(Cite as: 2006 WL 2990432 (N.D.Ill.))

H

United States District Court,
N.D. Illinois,
Eastern Division.
QSRSOFT, INC., Plaintiff,
v.
RESTAURANT TECHNOLOGY, INC., et al.,
Defendants.
No. 06 C 2734.

Oct. 19, 2006.

Jonathan Mandel Weis, Josh Slater Kaplan, Mitchell S. Chaban, Levin Ginsburg, Chicago, IL, for Plaintiff.

Darren Steven Cahr, David J. Moorhead, Gardner Carton & Douglas LLP, Chicago, IL, Jeanine Gibbs , Joseph D. Wargo, Julie C. Jared, Michael S. French, Wargo & French LLP, Atlanta, GA, for Defendants.

MEMORANDUM OPINION

SAMUEL DER-YEGHIAYAN, District Judge.

***1** This matter is before the court on Plaintiff QSRSoft, Inc.'s ("QSRSoft") motion for entry of a preliminary injunction against Defendant Restaurant Technology, Inc. ("RTI"). For the reasons stated below, we grant QSRSoft's motion for a preliminary injunction.

BACKGROUND

QSRSoft contends that every McDonald's Restaurant has a McDonald's Corporation computer system, an in store processor ("ISP"), that stores data about the restaurant's sales performance and status. McDonald's Corporation allegedly provides restaurant operators with limited reports, called R2D2, but in no relation to Star Wars, generated from the ISP data. Additionally, QSRSoft alleges that McDonald's Corporation has approved QSRSoft and RTI as back-office vendors, meaning that each has access to the data stored in the ISP. Both QSRSoft and RTI provide software tools to McDonald's Restaurant franchise owners and operators ("franchisees"). QSRSoft contends that both companies' software tools use data extracted from the ISP.

QSRSoft alleges that it developed the DotComm System, an internet-based computer system that assists franchisees in analyzing information collected from the restaurants. QSRSoft contends that the DotComm System differs from other competitors' systems in that it more quickly collects and processes information from restaurants, provides automatic information transfer backup, and provides underlying detail or reports. QSRSoft alleges that if a franchise wants to use the DotComm System, the franchisee must first obtain a licensing agreement, which includes a provision that only key management personnel are permitted to access the DotComm System due to its proprietary nature. According to QSRSoft, a franchisee is provided with the opportunity to evaluate the DotComm System for thirty days under the terms of a software evaluation licensing agreement. QSRSoft contends that once the franchisee agrees to the licensing agreement and identifies a list of the key personnel that will have access to the DotComm System, QSRSoft sends the franchisee an access code and unique password. QSRSoft alleges that the DotComm System automatically instructs the user to change the password during the first time the franchisee accesses the system. According to QSRSoft, the franchisee informs QSRSoft of the updated password.

QSRSoft claims that in January 2006, RTI, who provides predominantly accounting software to fast food restaurants, contacted F.A.F., Inc. d/b/a McDonald's Restaurant ("FAF"), which operates nine McDonald's restaurants in Fargo, North Dakota, to obtain information from QSRSoft about the DotComm System. QSRSoft contends that in

February 2006, Gregg Matejka ("Matejka"), FAF's director of operations, contacted QSRSoft about evaluating the DotComm System in one of FAF's McDonald's restaurants. QSRSoft claims that it subsequently sent a licensing agreement ("Agreement") to FAF and requested that the Agreement be executed and returned to QSRSoft. QSRSoft further alleges that on February 8, 2006, QSRSoft sent an access code and password to FAF in anticipation of receiving the executed Agreement from FAF. Although FAF did not return the Agreement, QSRSoft contends that FAF understood that FAF was accepting the terms of the Agreement and would use the DotComm System subject to such terms. QSRSoft claims that on February 8, 2006, FAF accessed the DotComm System using the newly provided access code and password, a process that required FAF to change the initial password. According to QSRSoft, on or about February 9, 2006, FAF provided RTI with the access code and the recently changed password ("FAF password").

***2** QSRSoft alleges that RTI used the FAF password from February 2006 until April 30, 2006 in order to gain access to the DotComm System, view, download, save, print, and copy each web page on the DotComm System, as well as to download the QSRSoft Data Engine, the backbone of the DotComm System's ability to extract restaurant information. QSRSoft claims that RTI was able to use the information it received from accessing the DotComm System to develop Reportsk, a similar RTI product for McDonald's franchises.

On August 8, 2006, QSRSoft filed an amended complaint that includes claims alleging copyright infringement under the Copyright Act of 1976, 17 U.S.C. 101 *et seq.* ("Copyright Act") brought against RTI (Count I), James H. Clutter ("Clutter") (Count II), and J. Neal Starkey ("Starkey") (Count III), claims alleging violations of the Illinois Trade Secret Act, 765 ILCS 1065/1 *et seq.*, ("ITSA") brought against RTI, Clutter, and Starkey (Count IV), conversion claims brought against RTI, Clutter, and Starkey (Count V), tortious interference with prospective business advantage claims brought against RTI, Clutter, and Starkey (Count VI), and tortious interference with contract claims brought against RTI, Clutter, and Starkey (Count VII).

On August 23, 2006, RTI filed a partial motion to dismiss Counts IV, V, and VII. On October 18, 2006 we denied RTI's partial motion to dismiss to the extent that it related to Counts IV and VII, and granted the motion to dismiss to the extent that it related to Count V. QSRSoft now seeks a preliminary injunction.

LEGAL STANDARD

A preliminary injunction "should not be granted unless the movant, by a clear showing, carries the burden of persuasion." *Goodman v. Ill. Dept. of Fin. & Prof'l Regulation,* 430 F.3d 432, 437 (7th Cir.2005)(stating that "[a]s the Supreme Court has observed, '[a] preliminary injunction is an extraordinary and drastic remedy" ')(quoting *Mazurek v. Armstrong,* 520 U.S. 968, 972 (1997)). When determining whether to use such a remedy, "the district [court] has to arrive at a decision based on a subjective evaluation of the import of the various factors and a personal, intuitive sense about the nature of the case." *Faheem-El v. Klincar,* 841 F.2d 712, 717 (7th Cir.1988)(quoting *Lawson Products, Inc. v. Avnet, Inc.,* 782 F.2d 1429, 1436 (7th Cir.1986)).

In order to obtain a preliminary injunction, a plaintiff must show that: "(1) [the plaintiff] ha[s] a reasonable likelihood of success on the merits; (2) no adequate remedy at law exists; (3) [the plaintiff] will suffer irreparable harm which, absent injunctive relief, outweighs the irreparable harm the respondent will suffer if the injunction is granted; and (4) the injunction will not harm the public interest." *Goodman,* 430 F.3d at 437. A likelihood of success means that the party has a "better than negligible chance" of succeeding on the merits. *Washington v. Ind. High Sch. Ath. Ass'n,* 181 F.3d 840, 845 (7th Cir.1999). Once the above four conditions are satisfied, the court evaluates the likelihood of success on a sliding scale. *AM General Corp. v. DaimlerChrysler Corp.,* 311 F.3d 796, 804 (7th Cir.2002). The factors in the sliding scale analysis include the irreparable harm the party

would endure without the preliminary injunction, any irreparable harm the opposing party will suffer as a result of the preliminary injunction, and any harm or benefit to the public if the injunction is granted or denied. *AM General Corp.,* 311 F.3d at 803-04; *Ty, Inc. v. Jones Group, Inc.,* 237 F.3d 891, 895 (7th Cir.2001). The sliding scale works in such a way that a lesser likelihood of success may support a preliminary injunction if the balance of harms favors the party seeking the remedy. *Ty,* 237 F .3d at 895; *Eli Lilly & Co. v. Natural Answers, Inc.,* 233 F.3d 456, 461 (7th Cir.2000). Likewise, a stronger likelihood of success permits granting a preliminary injunction even if the balance of harms is not necessarily in the seeking party's favor. *Bloedorn v.. Francisco Foods, Inc.,* 276 F.3d 270, 298 (7th Cir.2001).

DISCUSSION

I. Reasonable Likelihood of Success on the Merits

A. Copyright Claims

***3** Section 502(a) of the Copyright Act authorizes the court to issue a preliminary injunction "on such terms as [the court] may deem reasonable to prevent or restrain infringement of a copyright." 17 U.S.C. § 502(a). Irreparable injury may be presumed upon the showing of a *prima facie* case of copyright infringement. *Atari Inc. v. North Am. Philips Consumer Elec. Corp.,* 672 F.2d 607, 620 (7th Cir.1982). To prevail on a copyright infringement claim, QSRSoft must prove that (1) QSRSoft owned a valid copyright, and (2) RTI copied original elements, or infringement, of the work. *Feist Publ'ns, Inc. v. Rural Telephone Serv. Co., Inc.,* 499 U.S. 340, 361 (1991).

1. Copyright Validity

QSRSoft has registered copyrights in the Data Engine, Source Code, and QSRSoft Website. (P.Ex. 1). The Copyright Act provides that:

> In any judicial proceedings the certificate of a registration made before or within five years after first publication of the work shall constitute *prima facie* evidence of the validity of the copyright and of the facts stated in the certificate. The evidentiary weight to be accorded the certificate of a registration made thereafter shall be within the discretion of the court.

17 U.S.C. § 410(c). Since QSRSoft has provided Certificates of Registration for the Data Engine, Source Code, and QSRSoft Website ("Website") and each of the copyright registrations is within the past five years, the registrations are entitled by statute to a *prima facie* presumption of validity. *Id.* This presumption of validity and ownership is rebuttable. *Id.*

Although QSRSoft's registration certificates constitute *prima facie* evidence of validity, not every element of the copyrighted work is protected. Since the court must inquire as to what aspects of the work have been afforded copyright protection, it is not enough for QSRSoft to merely present the registration certificates. QSRSoft has failed to present evidence of the Data Engine and Source Code during the preliminary hearing or in its brief, but has introduced an example of the Website as Exhibit 1. Therefore, because QSRSoft has not presented sufficient evidence to support the likelihood of success on its copyright claims pertaining to the Data Engine and Source Code, we will only consider the copyright claim pertaining to the Website.

RTI argues that QSRSoft has failed "to show that it has an *original* work and not a mere compilation of unprotectable data ... [and has] failed to satisfy its burden." (Prelim.Inj.Resp.10)(emphasis in original). However, because proof of registration within five year after first publication of the work constitutes a *prima facie* presumption of validity, the burden does not fall upon QSRSoft to prove validity, but rather on RTI to rebut the presumption of copyright validity. 17 U.S.C. § 410(c). RTI contends that QSRSoft's copyrighted works are invalid because the Supreme Court in *Feist* has stated:

> ***4** Since facts do not owe their origin to an act of authorship, they are not original and, thus, are not copyrightable ... *copyright protection extends only to those components of the work that are original to the author, not to the facts themselves.*

(Prelim.Inj.Resp.10)(citing "*Feist,* 499 U.S. at 340 " [Syllabus]). The Syllabus of *Feist,* however, does

not constitute the opinion of the Supreme Court, but instead a summary of the case for the convenience of the researcher. *United States v.. Detroit Lumber Co.,* 200 U.S. 321, 337 (1905). Additionally, *Feist* does not stand for the proposition that a composition of facts are beyond copyright protection or that a compilation of facts requires more than a quantum of originality required to obtain a copyright in the work. *Feist,* 499 U.S. at 361. The *Feist* Court stated:

> Facts, whether alone or as part of a compilation, are not original and therefore may not be copyrighted. A factual compilation is eligible for copyright if it features an original selection or arrangement of facts, but the copyright is limited to the particular selection or arrangement. In no event may copyright extend to the facts themselves.

Id. at 351-52. Thus, while QSRSoft cannot copyright the ISP data, QSRSoft may copyright the manner in which it displays the data. Since the Data Engine and Source Code are not before this court, we are unable to determine the validity of those works. However, as stated above, a hardcopy of the QSRSoft Website was presented at the preliminary injunction hearing. (P Ex. 7). For the Website, QSRSoft does not contend to be copyrighting the ISP data, but does claim to be copyrighting the way in which it presents the data in the graphical displays. Accordingly, we find that there is sufficient evidence that shows that QSRSoft has met its burden to show a *prima facie* presumption of validity and RTI has not presented sufficient evidence to rebut such.

2. Copying of Original Expressions

The evidence presented during the preliminary injunction hearing indicates that QSRSoft is likely to prove the direct infringement of its works by RTI. The Copyright Act defines direct infringement as "[a]nyone who violates any of the exclusive rights of the copyright owner." 17 U.S.C. 501(a). The internet access logs demonstrate that RTI accessed the password protected copyrighted Website. The access logs also establish that RTI employees viewed, printed, and downloaded the information while viewing the Website. By downloading and printing the Website, RTI violated QSRSoft's exclusive right to reproduce the protected works. *See Marobie-Fl., Inc. v. National Ass'n of Fire Equip. Distribs.,* 983 F.Supp. 1167, 1173-74 (N.D.Ill.1997)(finding that downloading clip art constituted a violation of the plaintiff's right to reproduce its copyrighted work); *Sega Enterprises Ltd. v. Maphia,* 948 F.Supp. 923, 931-32 (N.D.Cal.1996)(finding that the new copies of a program were created upon uploading and downloading); *Playboy Enterprises, Inc. v. Frena,* 839 F.Supp. 1552, 1556 (M.D.Fla.1993)(finding that uploading files containing copyrighted photographs constituted reproduction).

***5** RTI argues that in order to prove that RTI infringed QSRSoft's copyrighted work the court must perform a "side-by-side" comparison of QSRSoft's product and RTI's product. RTI cites *Bridgmon v. Array Systems Corp.,* 325 F.3d 572 (5th Cir.2003), to support the need for a "side-by-side" comparison. In *Bridgmon,* the Fifth Circuit affirmed the granting of summary judgment because the plaintiff failed to produce evidence that would allow the court to do a "side-by-side" comparison. However, we decline to adopt *Bridgmon.* First, the *Bridgmon* court stated that "the law of [the Fifth] [C]ircuit prohibits finding copyright infringement without a sideby-side comparison of the two works," *id.* at 577, this court is not bound by the rulings of the Fifth Circuit. Second, the law of the Seventh Circuit, which is binding authority, does not require a "side-by-side" comparison of the products, but rather requires a substantial similarity between the plaintiff's copyrighted work and the defendant's work if there is no evidence of direct infringement. *Atari Inc.,* 672 F.2d at 614; *see Sassafras Enter. v. Roshco, Inc.,* 889 F.Supp 343 (N.D.Ill.1995)(noting that a side-by-side comparison is not required in the Seventh Circuit). Third, since there is a substantial likelihood of direct infringement, there is no need for this court to perform a substantial similarity test in this case. Fourth, *Bridgmon* occurred at the summary judgment stage of the proceeding, after completion of discovery, rather than during the preliminary injunction stage where discovery had not been completed and where the plaintiff would

have needed only to show a likelihood of success on the merits. Finally, because we are focused solely on the Website, we are able to perform the "ordinary observer" test applied in the Seventh Circuit. *Atari Inc.,* 672 F.2d at 614. Therefore, QSRSoft has a strong likelihood of showing that RTI copied original elements of the copyrighted Website.

B. Trade Secret Misappropriation

Under the ITSA, the court may issue an injunction if there is "actual or threatened misappropriation of a trade secret." 765 ILCS 1065/3(a). QSRSoft claims that RTI misappropriated "at least two of" its trade secrets: the Specific ISP Data and the 100k web-page displays ("Screen Shots"). (Mot.12). For QSRSoft to show a "better than negligible chance" on succeeding on its ITSA trade secret misappropriation claim, QSRSoft must show that (1) there is a trade secret; (2) the trade secret was misappropriated by RTI; and (3) RTI used the trade secret for business purposes. *See Composite Marine Propellers, Inc. v. Van Der Woude,* 962 F.2d 1263, 1265-66 (7th Cir.1992)(citing 765 ILCS 1065/2).

1. Existence of Trade Secrets

The ITSA defines a trade secret as:

> [I]nformation, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers, that:
> ***6** (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and
> (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.

765 ILCS 1065/2(d). The ITSA therefore "precludes trade secret protection for information generally known or understood within an industry even if not to the public at large," *Pope v. Alberto-Culver Co.,* 694 N.E.2d 615, 617 (Ill.App.Ct.1998), and "requires a plaintiff to take 'affirmative measures' to prevent others from using [the] information." *Jackson v. Hammer,* 653 N .E.2d 809, 816 (Ill.App.Ct.1995); *see Learning Curve Toys, Inc. v. PlayWood Toys, Inc.,* 342 F.3d 714, 722 (7th Cir.2003)(noting that the ITSA "prevents a plaintiff who takes no affirmative measures to prevent others from using its proprietary information from obtaining trade secret protection"). In determining whether a trade secret exists, Illinois courts generally look to: (1) the extent that the information is known outside of the business; (2) the extent that the information is known to employees and others within the business; (3) the measures taken to protect the information from outsiders; (4) the value of the information to competitors; (5) the amount of time, money, and effort to develop the information; and (6) the ease that the information could be acquired by others. *Learning Curve Toys,* 342 F.3d at 722. We disagree with RTI's contention that QSRSoft does not have any trade secret rights in the Specific ISP Data and Screen Shots.

The evidence shows that QSRSoft is likely to succeed in establishing the existence of valid trade secrets. First, although the ISP data is not stored on QSRSoft computers and the ISP data is owned by McDonald's franchisees, how QSRSoft compiles and manipulates the Specific ISP Data for use in the DotComm System is not known to competitors in the industry. Second, QSRSoft has taken reasonable measures to protect its trade secrets from the general public and competitors through the use of licensing agreements, a password protected website, and generally keeping its trade secrets out of the public display at conventions. *See Stampede Tool Warehouse, Inc. v. May,* 651 N.E.2d 209, 216 (Ill.App.Ct.1995)(finding that trade secret had not been waived when reasonable efforts were taken to protect secrecy of trade secrets from competitors). Third, QSRSoft has presented evidence that show it invested "over two and a half years, more than $2,000,000, and employed three full-time software developers and system architects" to develop the DotComm System. (Mot.13). Finally, due to the amount of data contained in the ISP, approximately 315 tables consisting of approximately one million pieces of information, and the fact that the Specific ISP Data represents approximately one percent of

the data in the ISP, competitors would have to spend a large amount of time and effort, just as QSRSoft has done, in order to ascertain the precise data needed to determine the Specific ISP Data.

*7 RTI contends that QSRSoft does not have valid trade secrets in the ISP Data or Screen Shots, noting that QSRSoft "spends only two of fifteen pages in its Motion discussing its alleged trade secret claim...." (Prelim.Inj.Resp.10). RTI argues that QSRSoft cannot show the validity of the QSRSoft trade secrets because QSRSoft never introduced either the Specific ISP Data or Screen Shots into evidence. RTI further states that QSRSoft "failed to put into evidence exactly what information [QSRSoft] is referring to when it refers to its Specific ISP Data and DotComm Screen Shots as trade secrets." (Prelim.Inj.Resp.11). In support of its argument, RTI contends that the Seventh Circuit in *Composite Marine Propellers, Inc.,* stated that *"[i]t is not enough to point to broad areas of technology and assert that something there must have been a secret and misappropriated* " and that *"[t]he plaintiff must show concrete secrets."* (Prelim.Inj.Resp.11)(emphasis in brief)(quoting 962 F.2d at 1265). In *Composite Marine Propellers,* however, the judge submitted the trade secret issues to the jury, rather than rule at the preliminary injunction stage. *Id.* at 1266. Additionally, RTI's brief and exhibits support the notion that QSRSoft did in fact show concrete trade secrets. First, RTI notes that "the DotComm product ... manipulates data that belongs to third [-]parties." (Prelim.Inj.Resp.2). This "manipulated data" is the Specific ISP Data trade secret referred to by QSRSoft. *See, e.g., ISC-Bunker Ramo Corp. v. Altech, Inc.,* 765 F.Supp. 1310 (N.D.Ill.1990) (finding technical manual compilations of information and procedures that were useful to financial institutions to be trade secrets under the ITSA). Second, the declaration of Barbra Morrison, (D.Ex.B), notes that she observed QSRSoft's "demonstration of its DotComm System on the big screen television" at the McDonald's Convention in May 2006. (D. Ex. B at 3). One cannot find a better way of pointing out concrete examples of the Screen Shots than on a big screen television. If at the trial stage QSRSoft is "vague about the nature of [its trade] secrets," then RTI's argument would be valid under Seventh Circuit precedent. (Prelim.Inj.Resp.11)(quoting *Composite Marine Propellers, Inc.,* 962 F.2d at 1266). However, at this stage of the proceedings, QSRSoft must only show that it has a better than negligible chance" of succeeding on the merits of its trade secret misappropriation claim, which includes showing the existence of trade secrets. *Washington,* 181 F.3d at 845.

RTI alternatively argues that QSRSoft did not reasonably maintain the secrecy of QSRSoft's trade secrets and QSRSoft thereby waived the trade secrets. RTI contends that in *Ruckelshaus v. Monsanto Co.,* 467 U.S. 986, 1002 (1984), "the United States Supreme Court has stated expressly that trade secrets are *extinguished* " when provided to a third-party that is not obligated to protect the confidentiality of the trade secrets." (Prelim.Inj.Resp.11)(emphasis in original). RTI contends that the Supreme Court has stated:

> ***8** Because of the intangible nature of a trade secret, the extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others. Information that is public knowledge or that is generally known in an industry cannot be a trade secret. *If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished.*

(Prelim.Inj.Resp.11)(citing *Ruckelshaus,* 467 U.S. at 1002)(emphasis in brief). However, in *Ruckelshaus,* the Supreme Court was faced with the question of whether the Takings Clause of the Fifth Amendment applied to the Environmental Protection Agency's ("EPA") public disclosure of a trade secret, an intangible property, in the same way it would to tangible property. 467 U.S. at 1001-02. The particular phrase cited by RTI was used by the Supreme Court to compare trade secrets to tangible property in finding that the plaintiff, Monsanto, had a property right that is protected by the Takings Clause since trade secrets have many of the characteristics of tangible property. *Id.* at 1001-04. Thus, the statement referred to by RTI is not a

"clear" statement that any disclosure to a third-party waives a trade secret, but rather is a general statement of the law. (Prelim.Inj.Resp.11).

RTI similarly cites *Skoog v. McCray Refrigerator Co.,* 211 F.2d 254, 257 (7th Cir.1954), stating that "[t]he Seventh Circuit has similarly found that the disclosure of a trade secret to those under no obligation to protect its confidentiality destroys the trade secret." (Prelim.Inj.Resp.11). However, *Skoog* is distinguishable from the instant action. In *Skoog,* the court found that the defendant could not misappropriate the trade secret at issue, a refrigerated cabinet, because the trade secret was no longer hidden from the public. 211 F.2d at 257-58. Specifically, the trade secret was extinguished because the plaintiff's refrigerated cabinet had been in unrestricted use in the plaintiff's grocery store, visible to anyone that entered the store, and the defendant had expressly stated that it did not accept the plaintiff's non-disclosure agreement. *Id.* In the instant action, the evidence establishes that QSRSoft's trade secrets were sufficiently guarded from the public. The efforts taken by QSRSoft to hide its trade secret from competitors such as RTI include: guarding the DotComm System with licensing agreements and a password protected website; not showing the Specific ISP Data or Data Engine to potential customers and competitors at conventions; typically only showing prospective customers and competitors less than five percent of the DotComm System at conventions; typically only showing prospective customers and competitors less than five percent of the Screen Shots at conventions; not showing the DotComm web interface during demonstrations; and not allowing customers and competitors to view the DotComm source code. These efforts are more than reasonable to establish a better than negligible chance that QSRSoft will be able to show that it did not waive its trade secrets. *See, e.g., Web Communications Group, Inc. v. Gateway 2000, Inc.,* 889 F.Supp. 316, 320 (N.D.Ill.1995)(holding that the plaintiff's trade secret misappropriation claim failed "because [plaintiff] took virtually no steps to protect the confidentiality" of the trade secret)(noting that none of the documents relating to the trade secret were marked as confidential (as was the plaintiff's policy with trade secrets), there was not a confidentiality agreement with the defendant, the plaintiff disclosed "either dummies or specifications" for the trade secret at issue to suppliers and competitors, and the plaintiff's president acknowledged that the competitor would be able to use the disclosed information for its own benefit); *Stampede Tool Warehouse,* 651 N.E.2d at 216 (finding that trade secret had not been waived when reasonable efforts were taken to protect secrecy of trade secrets from competitors); *cf. Skoog,* 211 F.2d at 257 (stating that it is "well established that there can be no confidential disclosure where there has been a prior disclosure to the *public without reservation* ")(emphasis added).

***9** RTI also argues that because an authorized user accessed the DotComm System and since QSRSoft did not immediately discontinue access to the DotComm System for that user, that QSRSoft has placed its trade secrets into the public domain. However, the evidence supports the finding that the only reported breach of QSRSoft's efforts to keep its trade secrets hidden was performed and traced back to RTI employees, Clutter and Starkey, who viewed, downloaded, and printed information while on the password protected website. *See* (P.Ex. 7, 8, 9, 10, 11)(showing internet access logs of alleged unauthorized users). Additionally, the fact that RTI understood that the DotComm System could only be accessed with the correct login information supports the claim that RTI was aware that QSRSoft had taken measures to protect its trade secrets. (D.Ex.D)(showing email from Matejka to Sten with DotComm access information). RTI's surreptitious access to the password protected website does not negate the fact that QSRSoft took reasonable efforts to protect its trade secrets. *Learning Curve Toys,* 342 F .3d at 725. Therefore, based on the evidence, we find that there is a strong likelihood that QSRSoft's claimed trade secrets are protected by the ITSA.

2. Trade Secret Misappropriation & Use of the Trade Secrets

The evidence also shows that QSRSoft has a strong likelihood of showing that RTI misappropriated

QSRSoft's trade secrets. The ITSA defines misappropriation as:

> (1) acquisition of a trade secret of a person by another person who knows or has reason to know that the trade secret was acquired by improper means; or
> (2) disclosure or use of a trade secret of a person without express or implied consent by another person who:
> (A) used improper means to acquire knowledge of the trade secret; or
> (B) at the time of disclosure or use, knew or had reason to know that knowledge of the trade secret was:
> (I) derived from or through a person who utilized improper means to acquire it;
> (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
> (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
> (C) before a material change of position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

765 ILCS 1065/2(b).

The internet access logs establish that RTI employees repeatedly accessed the DotComm System through the password protected website, viewed and printed the Screen Shots, and downloaded and saved the DotComm data archive containing historical FAF data that establishes the Specific ISP Data. Due to the amount of time and money expend by QSRSoft software developers and system architects to compile, manipulate, and solve the data contained in the ISP, coupled with the fact that there was no other product on the market that analyzed the data in such a way, at the very least, the information downloaded and saved by RTI served as a guide to RTI. Such a guide would have made it easier for RTI to develop Reportsk, a direct competitor to the DotComm System. Even if RTI did not directly copy QSRSoft's trade secrets, using the trade secrets as a guide likely rises to the level of misappropriation. *See Affiliated Hosp. Prods ., Inc. v. Baldwin,* 373 N.E.2d 1000, 1006 (Ill.App.Ct.1978)(stating that "even accepting their denial of any literal copying of [the] drawings, these drawings aided defendants in the design [of the infringing machinery], if only to demonstrate what pitfalls to avoid").

***10** Additionally, RTI's competing product, Reportsk, bears a strong resemblance to QSRSoft's DotComm System. First, both products use identical information, the Specific ISP Data contained within the ISP, to create reports for McDonald's franchisees. Second, the look and feel of the graphical summaries on the DotComm System's main page, (P Ex. 6), is nearly identical to RTI's brochure advertising Reportsk. (P Ex. 7). Third, the information listed on the DotComm System's main page is strikingly similar to RTI's brochure advertising Reportsk. Fourth, Matejka, who has used both products, testified that Reportsk "looked very similar to the QSRSoft Product ." (R. 47). These similarities exist despite the fact that RTI claims that "[t]he RTI Development Team did not download, use, or otherwise refer to [the] 'QSRSoft Data Engine,' including the source code associated with that engine ... in its development of the RTI Product." (D.Ex.A). RTI argues that "[t]he marketing brochure literally has nothing to do with the programming code for the RTI product." (Prelim.Inj.Resp.10). However, we do not find it plausible that RTI would distribute sales brochures that aim at attracting potential customers for a feature of the product that does not exist.

RTI argues that it could not misappropriate QSRSoft's trade secrets because RTI did not acquire the trade secrets through "improper means." (Prelim.Inj.Resp.1). The ITSA defines "improper means" to include "theft, bribery, misrepresentation, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means." 765 ILCS 1065/2(a). Evidence shows that RTI acquired access to the DotComm System password protected website by inducing FAF, through Matejka, to breach its confidential relationship with QSRSoft, as contained in the Agreement. According to Matejka, although he did not read the Agreement, he understood the Agreement to prohibit FAF from distributing the

password to anyone outside the FAF organization. (R. 44). FAF was bound by the Agreement once Matejka accessed the password protected website with the understanding that the password was not to be distributed to others outside of FAF. *See Wood v. Wabash County,* 722 N.E.2d 1176, 1179 (Ill.App.Ct.1999)(stating that an implied-in-fact contract is one in which an agreement may be inferred by performance of the parties). Thus, a confidential relationship existed between QSRSoft and FAF, and the evidence shows that RTI induced FAF to breach the confidential relationship.

RTI also contends that "[t]here is absolutely no evidence that RTI knew that FAF was not authorized" to send RTI access information for the DotComm System. (Prelim.Inj.Resp.11). However, this argument belies that RTI received the information from a FAF representative, rather than going directly to QSRSoft. In an email from Sten to Matejka, Sten requested specific information regarding the DotComm System, including sample reports, cost, internet speed, and timing. RTI could only acquire this information through a password protected website, which RTI could not access unless it signed a licensing agreement or received the information from FAF. Additionally, as stated above, RTI employees downloaded and saved the DotComm data archive containing historical FAF data that establishes the Specific ISP Data. RTI cannot claim that it did not know or understand that FAF was not authorized to send RTI access information for the password protected website of a potential competitor.

***11** Finally, RTI argues that "the very terms of [QSRSoft's] own License Agreement allow FAF to do exactly what it did in this case--disclose DotComm Products to a third-party (such as RTI)." We disagree. The Agreement states that:

> ... Licensee may *not* use the DotComm Product in a production environment, to produce revenue for Licensee, to demonstrate or provide Dotcomm Product to any other party or to develop software owned by any party other than QSRSoft.

(P.Ex. 3)(emphasis added). Although the licensing agreement may contemplate a breach of the Agreement, such a contemplation cannot be interpreted to mean that FAF could disclose the DotComm System to RTI. Therefore, the similarities between the DotComm System, combined with the unfettered access by RTI's employees to the DotComm System, as well as QSRSoft's alleged investment of "over two and a half years [and] more than $2,000,000 ...," (Mot.13), and RTI's relative lack of knowledge in this type of reporting system, as evidenced by RTI's need to access the DotComm System password protected website, give strong support to QSRSoft's claims of trade secret misappropriation and use of the trade secrets for business purposes by RTI.

II. Inadequate Remedy at Law & Irreparable Harm

There is a rebuttable presumption of irreparable harm to a plaintiff in cases of trade secret misappropriation and copyright infringement. *Atari Inc.,* 672 F.2d at 620; *ISC-Bunker Ramo Corp,* 765 F.Supp. at 1329. A defendant can rebut this presumption by demonstrating that the plaintiff will not suffer any harm if the injunction is not granted. *See Wainwright Secs., Inc. v. Wall Street Transcript Corp.,* 558 F.2d 91, 94 (2d Cir.1977)(explaining the rebuttable presumption). QSRSoft alleges that it has expended "over two and a half years, more than $2,000,000, and employed three full-time software developers and system architects" to develop the DotComm System. (Mot.13). QSRSoft claims that up until the point when QSRSoft introduced the DotComm System, there had not been a product on the market that similarly isolated and compiled the amount and type of data like the DotComm System. While RTI also has access to the ISP data and advertises to franchisees, RTI's expertise lies in accounting software which uses limited amounts of the ISP data. Even if QSRSoft were to succeed on its claims of copyright infringement and trade secret misappropriation, assessing the monetary value of QSRSoft's head start in the market would be nearly impossible. If RTI is allowed to market Reportsk to consumers, QSRSoft's head start will be lost and QSRSoft will be unable to reap the benefits as the initial market entrant, which would make assessing damages difficult. *See Ty,* 237 F.3d at 903 (stating that "it is virtually impossible to ascertain the precise economic consequences of intangible harms,

such as damage to reputation and loss of goodwill"); *Reinders Bros., Inc. v. Rain Bird E. Sales Corp.*, 627 F.2d 44, 53 (7th Cir.1980)(noting that damage to servicing clients efficiently constitutes irreparable harm). Additionally, RTI has failed to demonstrate that QSRSoft will not suffer any harm if the injunction is not granted and failed to note any harm that would come to RTI if the injunction is granted. Instead, RTI simply states that QSRSoft "offered absolutely no evidence of its alleged irreparable harm at the Evidentiary Hearing." (Prelim.Inj.Resp.15). Thus, we find that the balance of harms is clearly in favor of QSRSoft. Evidence establishes that QSRSoft is likely to prove material infringement in its copyright and trade secret misappropriation claims and the harm to RTI's potential sales of Reportsk is offset by the irreparable harm it may cause QSRSoft's business, reputation, and customer goodwill. QSRSoft also has shown no adequate remedy at law exists.

IV. Public Interest

***12** We find that granting an injunction is also in the public interest. The public is generally interested in upholding intellectual property rights, encouraging innovation and creativity, and rewarding those that take the risk and invest resources in pursuit of such innovation and creativity. *See generally,* United States Constitution, Art. I, sec. 8, cl. 8. Additionally, the public is unlikely to suffer any harm if RTI refrains from accessing, downloading, or copying the DotComm System. The public will also not suffer any harm if RTI is not allowed to destroy any materials that may be necessary to the instant matter, or if RTI is required to return the material that RTI acquired while accessing the DotComm System. Finally, since RTI has indicated that it "has no plan to offer the RTI Reportsk product during the pendency of this litigation" the public is unlikely to be harmed since Reportsk would not be on the market for sale. (D.Ex.B).

CONCLUSION

Based on the foregoing analysis, we grant QSRSoft's motion for a preliminary injunction.

Not Reported in F.Supp.2d, 2006 WL 2990432 (N.D.Ill.), 84 U.S.P.Q.2d 1297

END OF DOCUMENT